Before you Begin

This topic covers the prerequisites and limitations related to using the NITRO APIs.

Prerequisites

To use NITRO, you must have a basic understanding of the Citrix ADC appliance and you must make sure that the client application has one of the following:

- Access to a Citrix ADC appliance.
- To use REST APIs through HTTP, you must have a system to generate HTTP or HTTPS requests (payload in JSON format) to the Citrix ADC appliance. You can use any programming language or tool.
- For Java clients, you must have a system where Java Development Kit (JDK) 1.5 or later is available. The JDK can be downloaded from http://www.oracle.com/technetwork/java/javase/downloads/index.html.

  The NITRO library (available in <NITRO_SDK_HOME>/lib) must be installed on the client path. For installation instructions, read the <NITRO_SDK_HOME>/README.txt file.
- For .NET clients, you must have a system with .NET framework 3.5 or later installed. The .NET framework can be downloaded from http://www.microsoft.com/downloads/en/default.aspx.

  The NITRO library (available in <NITRO_SDK_HOME>/lib) must be installed on the client path. For installation instructions, read the <NITRO_SDK_HOME>/README.txt file.
- For Python clients, you must have a system with Python 2.7 or above version.

  The NITRO library (available in <NITRO_SDK_HOME>/lib) must be installed on the client path. For installation instructions, read the <NITRO_SDK_HOME>/README.txt file.

Obtaining the NITRO SDK Package

The NITRO package is available as a tar file on the Downloads page of the configuration utility of the Citrix ADC appliance. You must download and untar the file to a folder on your local system. This folder is referred to as \<NITRO_SDK_HOME\> in this documentation.

The folder contains the NITRO libraries in the lib subfolder. The libraries must be added to the client application classpath to access NITRO functionality. The \<NITRO_SDK_HOME\> folder also provides samples and documentation that can help you understand the NITRO SDK.

Limitations

The section lists the Citrix ADC operations that cannot be performed by using NITRO API.

`Note:` These operations can be performed on the Citrix ADC CLI or the GUI.

- install API and diff API on nsconfig resource
- UI-internal APIs (update, unset, and get)
- show ns info
- shutdown
- Application firewall API
- importwsdl
- importcustom
- importxmlschema
- importxmlerrorpage
- importhtmlerrorpage
- rmcustom
- rmxmlschema
- rmxmlerrorpage
- rmhtmlerrorpage
- CLI-specific API
- scp
- configaudit
- show defaults
- show permission
- batch
- source

NITRO Changes Across Releases

Some NITRO API have changed across releases. This topic details information which can help you avoid compatibility issues in your application.

Changes made from 13.1-4.4 -> 13.1-24.38

`Changes across NITRO flavors`:

The NITRO API changes that were made in release build 13.1-24.38 when compared with release build 13.1-4.4.

TYPE OF CHANGE	RESOURCE	METHOD/ATTRIBUTE
Attribute removed	nsfeature	htmlinjection
Attribute removed	nslicense	htmlinjection
Attribute removed	nstestlicense	htmlinjection
Attribute removed	cloud_stats	ngscgpicastart
Attribute removed	cloud_stats	ngscgpicastartrate
Attribute removed	cloud_stats	ngsgcticastart
Attribute removed	cloud_stats	ngsgcticastartrate
Attribute removed	cloud_stats	ngsshieldclxmtpconnestfailure
Attribute removed	cloud_stats	ngsshieldclxmtpconnestfailurerate
Attribute removed	cloud_stats	ngssocksicastart
Attribute removed	cloud_stats	ngssocksicastartrate
Attribute type changed	channel_interface_binding	lractiveintf

TYPE OF CHANGE	RESOURCE	METHOD/ATTRIBUTE
		Data type changed from Boolean to Integer.
Attribute type changed	Interface	lractiveintf Data type changed from Boolean to Integer.
Method removed	nsmigration	(nsmigration) get(nitro_service session)
Method removed	nsmigration	(nsmigration) get(options option, nitro_service session)
Method removed	urlfilteringcategorization	(urlfilteringcategorization) get(nitro_service session)
Method removed	urlfilteringcategorization	(urlfilteringcategorization) get(options option, nitro_service session)
Resource removed	wisite_translationinternalip_binding	-
Resource removed	wisite_farmname_binding	-
Resource removed	wisite_binding	-
Resource removed	wisite_accessmethod_binding	-
Resource removed	wisite	-
Resource removed	wipackage	-
Resource removed	wfsite	-
Resource removed	wfpackage	-

Changes made from 13.0-82.45 -> 13.1-4.4

`Changes across NITRO flavors`:

The NITRO API changes that were made in release build 13.1-4.4 when compared with release build 13.0-82.45.

`Note:` The following deprecated features have been removed and are no longer configurable from Citrix ADC version 13.1 onwards.

- SPDY, sure connect (SC), priority queuing (PQ), HTTP Denial of Service (DoS), and HTML Injection features.
- Filter feature (also known as Content Filtering or CF) - actions, policies, and binding.
- Classic policies and expressions. For more information, see Classic Policy Deprecation FAQs.

TYPE OF CHANGE	RESOURCE	METHOD/ATTRIBUTE
Attribute removed	crvserver_binding	crvserver_filterpolicy_binding
Attribute removed	csvserver_binding	csvserver_filterpolicy_binding
Attribute removed	nsfeature	hdosp
Attribute removed	nslicense	hdosp
Attribute removed	nstestlicense	hdosp
Attribute removed	lbvserver_binding	lbvserver_dospolicy_binding
Attribute removed	lbvserver_binding	lbvserver_filterpolicy_binding
Attribute removed	lbvserver_binding	lbvserver_pqpolicy_binding
Attribute removed	lbvserver_binding	lbvserver_scpolicy_binding
Attribute removed	lbvserver	pq

TYPE OF CHANGE	RESOURCE	METHOD/ATTRIBUTE
Attribute removed	nsfeature	pq
Attribute removed	nslicense	pq
Attribute removed	nstestlicense	pq
Attribute removed	crvserver	sc
Attribute removed	crvserver_appfwpolicy_binding	sc
Attribute removed	crvserver_cmppolicy_binding	sc
Attribute removed	csvserver	sc
Attribute removed	csvserver_appfwpolicy_binding	sc
Attribute removed	csvserver_auditnslogpolicy_binding	sc
Attribute removed	csvserver_auditsyslogpolicy_binding	sc
Attribute removed	csvserver_authorizationpolicy_binding	sc
Attribute removed	csvserver_cmppolicy_binding	sc
Attribute removed	lbvserver	sc
Attribute removed	lbvserver_appfwpolicy_binding	sc
Attribute removed	lbvserver_auditnslogpolicy_binding	sc
Attribute removed	lbvserver_auditsyslogpolicy_binding	sc

TYPE OF CHANGE	RESOURCE	METHOD/ATTRIBUTE
Attribute removed	lbvserver_authorizationpolicy_binding	sc
Attribute removed	lbvserver_cmppolicy_binding	sc
Attribute removed	nsfeature	sc
Attribute removed	nslicense	sc
Attribute removed	nstestlicense	sc
Attribute removed	server	sc
Attribute removed	server_servicegroup_binding	sc
Attribute removed	service	sc
Attribute removed	servicegroup	sc
Attribute removed	service_binding	service_dospolicy_binding
Attribute removed	service_binding	service_scpolicy_binding
Attribute removed	nshttpprofile	spdy
Attribute removed	protocolhttp_stats	spdyv3streamsrate
Attribute removed	protocolhttp_stats	spdyv2totstreams
Attribute removed	protocolhttp_stats	spdyv2streamsrate
Attribute removed	protocolhttp_stats	spdyv3totstreams
Attribute removed	protocolhttp_stats	spdytotstreams
Attribute removed	crpolicy	bindhits
Attribute removed	cspolicy	bindhits

TYPE OF CHANGE	RESOURCE	METHOD/ATTRIBUTE
Attribute removed	rewriteaction	bypasssafetycheck
Attribute removed	crpolicy	cspolicytype
Attribute removed	cspolicy	cspolicytype
Attribute removed	policydataset	description
Attribute removed	policyexpression	description
Attribute removed	policypatset	description
Attribute removed	crpolicy_crvserver_binding	domain
Attribute removed	crpolicy	domain
Attribute removed	cspolicy_crvserver_binding	domain
Attribute removed	cspolicy_cspolicylabel_binding	domain
Attribute removed	cspolicy_csvserver_binding	domain
Attribute removed	cspolicy	domain
Attribute removed	cmppolicy	expressiontype
Attribute removed	policydataset	indextype
Attribute removed	policypatset	indextype
Attribute removed	rewriteaction	pattern
Attribute removed	crpolicy_crvserver_binding	pihits
Attribute removed	cspolicy_csvserver_binding	pihits
Attribute removed	crpolicy_crvserver_binding	pipolicyhits
Attribute removed	cspolicy_csvserver_binding	pipolicyhits

TYPE OF CHANGE	RESOURCE	METHOD/ATTRIBUTE
Attribute removed	cmpglobal_cmppolicy_binding	policytype
Attribute removed	sslpolicy	policytype
Attribute removed	cmpglobal_cmppolicy_binding	state
Attribute removed	cspolicy_crvserver_binding	url
Attribute removed	cspolicy_cspolicylabel_binding	url
Attribute removed	cspolicy_csvserver_binding	url
Attribute removed	cspolicy	url
Attribute missing in method	lbvserver	sc and pq attributes are removed from the following method: (base_response) add(lbvserver obj, nitro_service session)
Attribute missing in method	lbvserver	sc and pq attributes are removed from the following method: (base_response) update(nitro_service session, lbvserver obj)
Attribute missing in method	service	sc attribute is removed from the following method: (base_response) add(nitro_service session, service obj)
Attribute missing in method	servicegroup	sc attribute is removed from the following method:

TYPE OF CHANGE	RESOURCE	METHOD/ATTRIBUTE
		(base_response) add(servicegroup obj, nitro_service session)
Attribute missing in method	service	sc attribute is removed from the following method: (base_response) update(service obj, nitro_service session)
Attribute missing in method	servicegroup	sc attribute is removed from the following method: (base_response) update(servicegroup obj, nitro_service session)
Attribute missing in method	nshttpprofile	spdy attribute is removed from the following method: (base_response) add(nshttpprofile obj, nitro_service session)
Attribute missing in method	nshttpprofile	spdy attribute is removed from the following method: (base_response) update(nitro_service session, nshttp profile obj)
Attribute missing in method	policyexpression	description attribute is removed from the following method: (base_response) add(policyexpression obj, nitro_service session)
Attribute missing in method	policyexpression	description attribute is removed from the following method:

TYPE OF CHANGE	RESOURCE	METHOD/ATTRIBUTE
		(base_response) update(policyexpression obj, nitro_service session)
Attribute missing in method	cspolicy	domain and url attributes are removed from the following method: (base_response) add(cspolicy obj, nitro_service session)
Attribute missing in method	policydataset	indextype attribute is removed from the following method: (base_response) add(nitro_service session, policydataset obj)
Attribute missing in method	policypatset	indextype attribute is removed from the following method: (base_response) add(policypatset obj, nitro_service session)
Attribute missing in method	rewriteaction	pattern and bypasssafetycheck attributes are removed from the following method: (base_response) add(rewriteaction obj, nitro_service session)
Attribute missing in method	rewriteaction	pattern and bypasssafetycheck attributes are removed from the following method:

TYPE OF CHANGE	RESOURCE	METHOD/ATTRIBUTE
		(base_response) update(nitro_service session, rewriteaction obj)
Attribute missing in method	cmpglobal_cmppolicy_binding	state attribute is removed from the following method: (base_response) add(cmpglobal_cmppolicy_binding obj, nitro_service session)
Attribute missing in method	cspolicy	url and domain attributes are removed from the following method: (base_response) update(nitro_service session, cspolicy obj)
Resource removed	crvserver_filterpolicy_binding	-
Resource removed	csvserver_filterpolicy_binding	-
Resource removed	dos_stats	-
Resource removed	dospolicy_stats	-
Resource removed	dospolicy	-
Resource removed	filteraction	-
Resource removed	filterglobal_binding	-
Resource removed	filterglobal_filterpolicy_binding	-
Resource removed	filterhtmlinjectionparameter	-

TYPE OF CHANGE	RESOURCE	METHOD/ATTRIBUTE
Resource removed	filterhtmlinjectionvariable	-
Resource removed	filterpolicy_binding	-
Resource removed	filterpolicy_csvserver_binding	-
Resource removed	filterpolicy_filterglobal_binding	-
Resource removed	filterpolicy_lbvserver_binding	-
Resource removed	filterpolicy	-
Resource removed	filterpostbodyinjection	-
Resource removed	filterprebodyinjection	-
Resource removed	lbvserver_dospolicy_binding	-
Resource removed	lbvserver_filterpolicy_binding	-
Resource removed	lbvserver_pqpolicy_binding	-
Resource removed	lbvserver_scpolicy_binding	-
Resource removed	pq_stats	-
Resource removed	pqbinding_args	-
Resource removed	pqbinding	-
Resource removed	pqpolicy_stats	-
Resource removed	pqpolicy	-
Resource removed	sc_stats	-

TYPE OF CHANGE	RESOURCE	METHOD/ATTRIBUTE
Resource removed	scparameter	-
Resource removed	scpolicy_stats	-
Resource removed	scpolicy	-
Resource removed	service_dospolicy_binding	-
Resource removed	service_scpolicy_binding	-

Changes made from 13.0-52.24 -> 13.0-76.31

- `Changes across NITRO flavors`

  The NITRO API changes that were made in release build 13.0-76.31 when compared with release build 13.0-52.24.

`Note:` Resources and attributes related to Cisco RISE feature have been removed.

TYPE OF CHANGE	RESOURCE	METHOD/ ATTRIBUTE	REMARKS
Attribute removed	vpnvserver	analyticsprofile	In 13.0-76.31 and later builds, multiple analytics profiles can be associated. vpnvserver_analyticsprofile_binding resource has been added for this purpose.
Attribute removed	appfwprofile	autodeployrule	-
Attribute removed	appflowparam	aaainsight	If API Gateway license and feature

TYPE OF CHANGE	RESOURCE	METHOD/ ATTRIBUTE	REMARKS
			are enabled, transactions with content-type as application/json are included in the appflow records by default.
Attribute type changed	policyevaluation	pitoffsetlengtharray	Attribute type has changed from integer to double.

Changes made from 12.1-48.13 -> 13.0-52.24

`Changes across NITRO flavors`:

The NITRO changes that were made in release 13.0-52.24 when compared with release 12.1-48.13.

TYPE OF CHANGE	RESOURCE	METHOD/ ATTRIBUTE	REMARKS
Attribute removed	rnat	rnatip2	In 12.1 and earlier releases, for creating or updating ACL based RNAT resources, `natip2` attribute was used. This has been changed to `natip` attribute for making it consistent with network based RNAT resources, get and update.
Attribute type changed	rnat	redirectport	Data type for `redirectport` attribute is changed

TYPE OF CHANGE	RESOURCE	METHOD/ ATTRIBUTE	REMARKS
			from boolean to integer.
Attribute missing in method	rnat	clear(), redirectport, natip	`redirectport` and `natip` attributes are removed from clear() operation. Also, the `clear()` operation is deprecated, Use `delete()` operation instead.
Attribute missing in method	rnat	unset(), ownergroup, redirectport	-
Attribute missing in method	Authenticationpushservice	POST/PUT, namespace	The `namespace` attribute is set to a constant value of `https://mfa.cloud.com`. This attribute cannot be modified.
Attribute removed	vpnvserver	policy, priority, gotopriorityexpression	These attributes are removed from `vpnvserver` resource because these attributes are related to `policy binding`.

- `Changes specific to NITRO SDKs`

  The SDK-specific changes that were made in release 13.0-52.24 when compared with release 12.1-48.13.

TYPE OF CHANGE	CLASS	METHOD/ ATTRIBUTE	REMARKS
Method removed	systemfile	(systemfile[]) get(nitro_service session), (systemfile[]) get(options option, nitro_service session), (systemfile) get(String filename, nitro_service session)	These methods were not useful because `filelocation` was always a required attribute in fetching system files.
Attribute type changed	nsconnectiontable	irs, iss	Data type changed from `Integer` to `Double`.
Method removed	nsvpxparam	(nsvpxparam) get(nitro_service session)	With cluster support for `nsvpxparam`, the `get()` method returns an array instead of single entity.
Method removed	nsconfig	(base_response) save(nitro_service session)	Alternate method - 'base_response save(nitro_service client, nsconfig resource)'
Attribute type changed	appfwprofile	postbodylimit	datatype changed from uint? to long?

Changes made from 12.0-57.24 -> 12.1-48.13

- `Changes across NITRO flavors`

  The NITRO changes that were made in release 12.1-48.13 when compared with release 12.0-57.24.

TYPE OF CHANGE	RESOURCE	METHOD/ ATTRIBUTE	REMARKS
Attribute removed	nsicapprofile	insertxserverip, insertxclientip, sendreqinresmod, insertxauthuseruri, onservererrorresponse	-
Attribute removed	lsnclient	td	“td” is applicable to lsnclientonly in conjunction with network/network6. This attribute is now a part of lsnclient_network_binding and lsclient_netwrok6_binding resources.
Attribute removed	nspartition_stats	minbandwidth	minbandwidth setting on the partition is deprecated.
Attribute removed	cloudparameter	verifyurl	This attribute is renamed to activationcode.
Attribute removed	appfwprofile_safeobject_binding	expression	This attribute is renamed to as_expression.

- `Changes specific to NITRO SDKs`

  The SDK-specific changes that were made in release 12.1-48.13 when compared with release 12.0-57.24.

TYPE OF CHANGE	CLASS	METHOD/ ATTRIBUTE	REMARKS
Method removed	nsacls	(base_response) renumber(nitro_service session)	Alternate method - (base_response)renumber(nitro_service client, nsacls resource)
Method removed	nsacls	(base_response) clear(nitro_service session)	Alternate method - (base_response)clear(nitro_service client, nsacls resource)
Method removed	nsacls	(base_response) apply(nitro_service session)	Alternate method - (base_response)apply(nitro_service client, nsacls resource)
Method removed	nsacls6	(base_response) renumber(nitro_service session)	Alternate method - (base_response)renumber(nitro_service client, nsacls6 resource)
Method removed	nsacls6	(base_response) clear(nitro_service session)	Alternate method - (base_response)clear(nitro_service client, nsacls6 resource)
Method removed	nsacls6	(base_response) apply(nitro_service session)	Alternate method - (base_response)apply(nitro_service client, nsacls6 resource)

Performing Basic Citrix ADC Operations

This section covers procedures for performing the following basic Citrix ADC operations using NITRO APIs.

- Log on to a Citrix ADC Appliance
- Log on to a Citrix ADC appliance that has two factor authentication configured for system users
- Enable Citrix ADC Features and Modes
- Save Citrix ADC Configurations
- Kill a system Session
- Disconnect from the Citrix ADC Appliance

Log on to a Citrix ADC Appliance

The first step towards using NITRO is to establish a session with the Citrix ADC appliance and then authenticate the session by using the Citrix ADC administrator's credentials.

Some points to note with regards to session timeout:

- When restricted timeout param is enabled, NITRO, by default, uses the timeout value that is configured for the logged in user. You can customize this value but it must be limited to the value specified for the user. If no value is specified for the user, the default timeout value of 15 minutes is used.
- When restricted timeout param is not enabled, NITRO uses the default value of 30 minutes as session timeout.
- `Using REST APIs through HTTP`

  You must specify the username and password in the login object. The session ID that is created must be specified in the request header of all further operations in the session.

`Notes:`

- You must have a user account on the appliance to log on to it. The configuration operations that you can perform are limited by the administrative roles assigned to your account.

- To ensure secure communication, use the HTTPS protocol in NITRO requests.
- Instead of creating a NITRO session, you can log on to the Citrix ADC appliance while performing individual operations. To do this, you must specify the username and password in the request header of the NITRO request as follows:
  - X-NITRO-USER:<username\>
  - X-NITRO-PASS:<password\>
  - Content-Type:application/json

For example, to connect and create a session with a Citrix ADC appliance with NSIP address 10.102.29.60 by using the HTTP protocol:

- `Request`

  `HTTP Method:` POST

`URL:` http://10.102.29.60/nitro/v1/config/login

`Request Headers:` Content-Type:application/json

`Request Payload:`

```
{

    "login":

    {

    "username":"admin",

    "password":"verysecret"

    }

}
```

- `Response`

  `HTTP Status Code on Success:` 201 Created

`HTTP Status Code on Failure:` 4xx <string> (for general HTTP errors) or 5xx <string> (for Citrix-ADC-specific errors). The response payload provides details of the error.

`Response Header:`

```
Set-Cookie:NITRO_AUTH_TOKEN=<tokenvalue>;

path=/nitro/v1
```

- `Using REST APIs through SDKs`

  You must create an object of the com.citrix.netscaler.nitro.service.nitro_service class by specifying the Citrix ADC IP (NSIP) address and the protocol to connect to the appliance (HTTP or HTTPS). You then use this object and log on to the appliance by specifying the user name and the password of the Citrix ADC administrator.

`Note:`

- For the python SDK, the package path is of the form nssrc.com.citrix.netscaler...
- You must have a user account on that appliance. The configuration operations that you perform are limited by the administrative roles assigned to your account.

The following sample code establishes a session with a Citrix ADC appliance with IP address 10.102.29.60 by using the HTTPS protocol and also sets a session timeout period (in seconds) of 60 minutes.

`Java - Sample code to establish session`

```
//Specify the Citrix ADC appliance IP address and protocol

nitro_service ns_session = new nitro_service("10.102.29.60","https");



//Specify the login credentials

ns_session.login("admin","verysecret",3600);
```

`.NET - Sample code to establish session`

```
//Specify the Citrix ADC appliance IP address and protocol

nitro_service ns_session = new nitro_service("10.102.29.60","https");
```

```
//Specify the login credentials

ns_session.login("admin","verysecret",3600);
```

`Python - Sample code to establish session`

```
# Specify the Citrix ADC appliance IP address and protocol

ns_session = nitro_service("10.102.29.60","https")

# Specify the login credentials

ns_session.login("admin","verysecret",3600)
```

Disable SSL Checks

When using HTTPS, you must make sure that the root CA is added to the truststore. By default, NITRO validates the SSL certificate and verifies the hostname.

- `Using REST APIs through SDKs`

  Disable these validations as shown in the following sample codes.

`Java - Sample code for disabling SSL checks`

```
ns_session.set_certvalidation(false);

ns_session.set_hostnameverification(false);
```

`.NET - Sample code for disabling SSL checks`

```
ns_session.certvalidation = false;

ns_session.hostnameverification = false;
```

`Python - Sample code for disabling SSL checks`

```
ns_session.certvalidation = false
```

Log on to a Citrix ADC appliance that has two factor authentication configured for system users

Two factor authentication is a security mechanism where a Citrix ADC appliance authenticates a system user at two authenticator levels. The appliance grants access to the user only after successful validation of passwords by both levels of authentication.

For information about configuring two factor authentication for system users by using Citrix ADC CLI or GUI, see Two factor authentication for system users.

Steps to log on to a Citrix ADC appliance that has two factor authentication configured

1. Send user credentials for the first level authentication
2. Send user credentials for the second level authentication

Send user credentials for the first level authentication

You use the `login` API object to send the username and first password to the Citrix ADC appliance for first level authentication.

The Citrix ADC appliance responds with a session (token) ID, error code, a next factor login message, and other details. The error code and next factor login message indicates that a second level authentication is required to complete the login process.

Request structure

REQUEST FIELD	VALUE
HTTP Method	`POST`

REQUEST FIELD	VALUE
URL	`http://<Citrix-ADC-IP-address(NSIP)>/nitro/v1/config/login`
Request Headers	`Content-Type: application/x-www-form-urlencoded`
Request Payload	`{"login":{"username":"<username>","password":"<first password>"}}`

Send user credentials for the second level authentication

You use the `loginnextfactorresponse` API object to send the following information to the Citrix ADC appliance for second level authentication.

- Second password (next factor password)
- Session ID (received as part of first level authentication)

The Citrix ADC appliance responds with an error code, a message, and other details. An error code of `0` and a message of `Done` indicate that the two factor authentication process is completed with success. The session ID received must be specified in the request header of all further operations in the session.

Request structure

REQUEST FIELD	VALUE
HTTP Method	`POST`
URL	`http://<Citrix-ADC-IP-address(NSIP)>/nitro/v1/config/loginnextfactorresponse`
Request Headers	`Content-Type: application/x-www-form-urlencoded`
Request Payload	`{"loginnextfactorresponse":{"nextfactorpassword":"<second password>","sessionid":"<session id>"}}`

Sample configuration

STEPS	CURL REQUESTS	RESPONSE
Send user credentials for the first level authentication	`curl -X POST -H "Content-Type:application/json" http://10.102.29.30/nitro/v1/config/login -d '{"login":{"username":"exampleusername","password":"examplepassword"}}'`	`{"errorcode": 3816, "message": "Nextfactor Login [singleauth_password]", "severity": "ERROR", "sessionid":"##73EF2C4487554615539D52FDAAF5D1"}`
Send user credentials for the second level authentication	`curl -X POST -H "Content-Type:application/json" http://192.0.0.33/nitro/v1/config/loginnextfactorresponse -d '{"loginnextfactorresponse":{"nextfactorpassword":"examplesecondpassword"},"sessionid":"##73EF2C4487554615539D52FDAAF5D1"}'`	`{ "errorcode": 0, "message": "Done", "severity": "NONE", "sessionid": "##73EF2C4487554615539D52FDAAF5D1" }`

Enabling Citrix ADC Features and Modes

Some Citrix ADC features and modes are disabled by default and therefore must be enabled before they can be configured. To enable a Citrix ADC feature or mode, specify the action as "enable" in the URL query string, and in the request payload, specify the feature or mode to be enabled.

- `Using REST APIs through HTTP`

  To disable a feature or mode, in the URL query string, specify the action as "disable".

For example, to enable the load balancing and content switching features:

- `Request`

`HTTP Method:` POST

`URL:` http://<Citrix-ADC-IP-address(NSIP)>/nitro/v1/config/nsfeature?action=enable

`Request Headers:`

Cookie:NITRO_AUTH_TOKEN=<tokenvalue>

Content-Type:application/json

`Request Payload:`

```
{
    "nsfeature":
    {
        "feature":
        [
            "LB",
            "CS"
        ]
    }
}
```

- `Response`

  `HTTP Status Code on Success:` 200 OK

`HTTP Status Code on Failure:` 4xx <string> (for general HTTP errors) or 5xx <string> (for Citrix-ADC-specific errors). The response payload provides details of the error.

To enable the L2 and fast ramp modes:

- `Request`

  `HTTP Method:` POST

`URL:` http://<Citrix-ADC-IP-address(NSIP)>/nitro/v1/config/nsmode?action=enable

`Request Headers:`

Cookie:NITRO_AUTH_TOKEN=<tokenvalue>

Content-Type:application/json

`Request Payload:`

```
{
    "nsmode":
    {
        "mode":
        [
            "L2",
            "FR"
        ]
    }
}
```

- `Response`

  `HTTP Status Code on Success:` 200 OK

`HTTP Status Code on Failure:` 4xx <string> (for general HTTP errors) or 5xx <string> (for Citrix-ADC-specific errors). The response payload provides details of the error.

Saving Citrix ADC Configurations

To make sure that the configurations persist on rebooting the appliance, you must save the Citrix ADC configurations. To save the configurations, specify the action as "save" in the URL query string.

- `Using REST APIs through HTTP`

  To save the configurations:

- `Request`

  `HTTP Method:` POST

`URL:` http://<Citrix-ADC-IP-address(NSIP)>/nitro/v1/config/nsconfig?action=save

`Request Headers:`

Cookie:NITRO_AUTH_TOKEN=<tokenvalue>

Content-Type:application/json

`Request Payload:`

```
{

    "nsconfig":

    {}

}
```

- `Response`

  `HTTP Status Code on Success:` 200 OK

`HTTP Status Code on Failure:` 4xx <string> (for general HTTP errors) or 5xx <string> (for Citrix-ADC-specific errors). The response payload provides details of the error.

Killing a System Session

A Citrix ADC administrator can kill any system session by specifying the action as "kill" in the URL query string and by specifying the required system session ID in the request payload.

- `Using REST APIs through HTTP`

  For example, to kill a system session that has ID as 311:

- `Request`

  `HTTP Method:` POST

`URL:` http://<Citrix-ADC-IP-address(NSIP)>/nitro/v1/config/systemsession?action=kill

`Request Headers:`

Cookie:NITRO_AUTH_TOKEN=<tokenvalue>

Content-Type:application/json

`Request Payload:`

```
{
    "systemsession":
    {
    "sid":"311"
    }
}
```

- `Response`

  `HTTP Status Code on Success:` 200 OK

`HTTP Status Code on Failure:` 4xx <string> (for general HTTP errors) or 5xx <string> (for Citrix-ADC-specific errors). The response payload provides details of the error.

Disconnecting from the Citrix ADC Appliance

Before disconnecting (logging out) from the Citrix ADC appliance, make sure that you have saved the Citrix ADC configurations.

- `Using REST APIs through HTTP`

  To logout of the Citrix ADC appliance:

- `Request`

  `HTTP Method:` POST

`URL:` http://<Citrix-ADC-IP-address(NSIP)>/nitro/v1/config/logout

`Request Headers:`

Cookie:NITRO_AUTH_TOKEN=<tokenvalue>

Content-Type:application/json

`Request Payload:`

```
{

    "logout":{}

}
```

- `Response`

  `HTTP Status Code on Success:` 201 Created

`HTTP Status Code on Failure:` 4xx <string> (for general HTTP errors) or 5xx <string> (for Citrix-ADC-specific errors). The response payload provides details of the error.

Performing Citrix ADC Resource Operations

Citrix ADC resources are organized into a set of packages or namespaces. Each package or namespace corresponds to a Citrix ADC feature. For example, all load-balancing related resources, such as load balancing virtual server, load balancing group, and load balancing monitor are available in com.citrix.netscaler.nitro.resource.config.lb.

Similarly, all application firewall related resources, such as application firewall policy and application firewall archive are available in com.citrix.netscaler.nitro.resource.config.appfw.

Each Citrix ADC resource is represented by a class. For example, the class that represents a load balancing virtual server is called lbvserver (in com.citrix.netscaler.nitro.resource.config.lb). The state of a resource is represented by properties of a class. You can get and set the properties of the class.

The setter and getter properties are always executed locally on the client. They do not involve any network interaction with the NITRO web service. All properties have basic simple types: integer, long, boolean, and string.

Adding a Citrix ADC Resource

This topic covers adding a Citrix ADC resource by using REST APIs through HTTP or SDKs.

- `Using REST APIs through HTTP`

  To create a new resource (for example, an lbvserver) on the appliance, specify the resource name and other related arguments in the specific resource object.

For example, to create an load balancing virtual server named MyFirstLbVServer:

- `Request`

  `HTTP Method:` POST

`URL:` http://<Citrix-ADC-IP-address(NSIP)>/nitro/v1/config/lbvserver

`Request Headers:`

Cookie:NITRO_AUTH_TOKEN=<tokenvalue>

Content-Type:application/json

`Request Payload:`

```
{

    "lbvserver":

    {

    "name":"MyFirstLbVServer",

    "servicetype":"http"

    }

}
```

- `Response`

  `HTTP Status Code on Success:` 201 Created

`HTTP Status Code on Failure:` 4xx <string> (for general HTTP errors) or 5xx <string> (for Citrix-ADC-specific errors). The response payload provides details of the error.

- `Using REST APIs through SDKs`

  To create a new resource, instantiate the resource class, configure the resource by setting its properties locally, and then upload the new resource instance to the Citrix ADC appliance.

The following sample code creates a load balancing virtual server.

`Java - Sample code to add a Citrix ADC resource`

```
//Create an instance of the lbvserver class



lbvserver new_lbvserver_obj = new lbvserver();



//Set the properties of the resource locally
```

```
new_lbvserver_obj.set_name("MyFirstLbVServer");
new_lbvserver_obj.set_ipv46("10.102.29.88");
new_lbvserver_obj.set_port(88);
new_lbvserver_obj.set_servicetype("HTTP");
new_lbvserver_obj.set_lbmethod("ROUNDROBIN");

//Upload the resource to Citrix ADC

lbvserver.add(ns_session,new_lbvserver_obj);
```

`.NET - Sample code to add a Citrix ADC resource`

```
//Create an instance of the lbvserver class

lbvserver new_lbvserver_obj = new lbvserver();

//Set the properties of the resource locally

new_lbvserver_obj.name = "MyFirstLbVServer";
new_lbvserver_obj.ipv46 = "10.102.29.88";
new_lbvserver_obj.port = 88;
new_lbvserver_obj.servicetype = "HTTP";
```

```
new_lbvserver_obj.lbmethod = "ROUNDROBIN";


//Upload the resource to Citrix ADC


lbvserver.add(ns_session,new_lbvserver_obj);
```

`Python - Sample code to add a Citrix ADC resource`

```
# Create an instance of the lbvserver class


new_lbvserver_obj = lbvserver()


# Set the properties of the resource locally


new_lbvserver_obj.name = "MyFirstLbVServer"

new_lbvserver_obj.ipv46 = "10.102.29.88"

new_lbvserver_obj.port = 88

new_lbvserver_obj.servicetype = "HTTP"

new_lbvserver_obj.lbmethod = "ROUNDROBIN"


# Upload the resource to CItrix ADC
```

```
lbvserver.add(ns_session, new_lbvserver_obj)
```

Enabling a Citrix ADC Resource

This topic covers enabling a Citrix ADC resource by using REST APIs through HTTP or SDKs.

- `Using REST APIs through HTTP`

  To enable a resource on the Citrix ADC appliance, specify the action as "enable" in the URL query string, and in the request payload, specify the resource to be enabled. To disable a resource, in the URL query string, specify the action as "disable".

For example, to enable a load balancing virtual server named MyFirstLbVServer.

- `Request`

  `HTTP Method:` POST

`URL:` http://<Citrix-ADC-IP-address(NSIP)>/nitro/v1/config/lbvserver?action=enable

`Request Headers:`

Cookie:NITRO_AUTH_TOKEN=<tokenvalue>

Content-Type:application/json

`Request Payload:`

```
{

    "lbvserver":

    {

    "name":"MyFirstLbVServer"

    }

}
```

- `Response`

`HTTP Status Code on Success:` 200 OK

`HTTP Status Code on Failure:`

4xx <string> (for general HTTP errors) or 5xx <string> (for Citrix-ADC-specific errors). The response payload provides details of the error.

- `Using REST APIs through SDKs`

  To enable a resource, invoke the enable() method and to disable, invoke the disable() method.

The following sample code enables a load balancing virtual server named lb_vip.

`Java - Sample code to enable a Citrix ADC resource`

```
lbvserver obj = new lbvserver();



obj.set_name("lb_vip");



lbvserver.enable(ns_session, obj);
```

`.NET - Sample code to enable a Citrix ADC resource`

```
lbvserver obj = new lbvserver();



obj.name = "lb_vip";



lbvserver.enable(ns_session, obj);
```

`Python - Sample code to enable a Citrix ADC resource`

```
obj = lbvserver()
```

```
obj.name = "lb_vip"



lbvserver.enable(ns_session, obj)
```

Retrieving Properties of Citrix ADC Resources

This topic covers retrieving properties of a Citrix ADC resource by using REST APIs through HTTP or SDKs.

- `Using REST APIs through HTTP`

  NITRO provides multiple approaches using which you can retrieve resources and their relevant details. The following table explains each of these approaches with the required URL.

Retrieving all details of all resources of a specific type	In the URL, specify the type of resource for which you want to retrieve the details. For example, to retrieve all details of load balancing virtual servers available on a Citrix ADC appliance. http://<Citrix-ADC-IP-address(NSIP)>/nitro/v1/config/lbvserver
Retrieving all details of a specific resource	In the URL, specify the name of resource for which you want to retrieve the details. For example, to retrieve all details of a load balancing virtual server named MyFirstLbVServer: http://<Citrix-ADC-IP-address(NSIP)>/nitro/v1/config/lbvserver/MyFirstLbVServer
Retrieving summary or detailed view of resources	In the URL, use the "view" query parameter to specify whether you want to view the

	summary (mandatory parameters) or detail (all parameters). For example, to view the mandatory parameters for all load balancing virtual servers: http://<Citrix-ADC-IP-address(NSIP)>/nitro/v1/config/lbvserver?view=summary Note: By default, the retrieved results are displayed in detail view (?view=detail).
Retrieving all details of resources that have multiple unique identifiers	In the URL, specify the type of resource and use the "args" query parameter to specify the unique attributes and the values for those attributes. For example, to get the application firewall profiles that have unique identifiers "name" and "starturl" as appfw1 and aa respectively. http://<Citrix-ADC-IP-address(NSIP)>/nitro/v1/config/appfwprofile?args=name:appfw1,starturl:aa
Retrieving specific details of all resources of a specific type	In the URL, specify the type of the resource and use the "attrs" query parameter to specify the resource details that you want to retrieve. For example, to retrieve the "name" and "lbmethod" of all load balancing virtual servers: http://<Citrix-ADC-IP-address(NSIP)>/nitro/v1/config/lbvserver?attrs=name,lbmethod
Retrieving specific details of a specific resource	In the URL, specify the type and name of the resource and use the "attrs" query parameter

	to specify the resource details that you want to retrieve. For example, to retrieve the "name" and "lbmethod" of a load balancing virtual server named "MyFirstLbVServer": http://<Citrix-ADC-IP-address(NSIP)>/nitro/v1/config/lbvserver/MyFirstLbVServer?attrs=name,lbmethod
Filtering the retrieved resources	In the URL, specify the type of resource and use the "filter" query parameter to specify the attribute(s) and the value(s) of the attributes. The resources fetched will be filtered based on the filter criteria. Note: The filter query parameter supports the use of PCRE regular expressions. For example, to filter the load balancing virtual servers where the "lbmethod" is ROUNDROBIN. http://<Citrix-ADC-IP-address(NSIP)>/nitro/v1/config/lbvserver?filter=lbmethod:ROUNDROBIN
Retrieving resources in paginated manner	If the request is likely to result in a large number of resources, you can divide the results into pages and retrieve them page by page (paginated). For example, if you are retrieving all the 53 load balancing virtual servers of a Citrix ADC appliance, instead of retrieving all 53 in one response, you can configure the results to be divided into 6 pages each having 10 results. In the URL, specify the name of the resource and use the following query parameters:

	• "pageno" - The page number to be displayed. • "pagesize" - The number of resources to be displayed in each page. For example, to retrieve the load balancing virtual servers in a paginated form, first get a count (using the "count" query parameter shown in below row) of the load balancing virtual servers. Then, accordingly specify the number of results for each page and then specify the page number to be displayed. http://<Citrix-ADC-IP-address(NSIP)>/nitro/v1/config/lbvserver?pagesize=10&pageno=3

For example, to retrieve only the name and load balancing method of all load balancing virtual servers on a Citrix ADC.

- `Request`

  `HTTP Method:` GET

`URL:` http://<Citrix-ADC-IP-address(NSIP)>/nitro/v1/config/lbvserver?attrs=name,lbmethod

`Request Headers:`

Cookie:NITRO_AUTH_TOKEN=<tokenvalue>

Accept:application/json

- `Response`

  `HTTP Status Code on Success:` 200 OK

`HTTP Status Code on Failure:`

4xx <string> (for general HTTP errors) or 5xx <string> (for Citrix-ADC-specific errors). The response payload provides details of the error.

`Response Header:`

Content-Type:application/json

`Response Payload:`

```
{
    lbvserver:
    {
        name: "test",
        lbmethod: "LEASTCONNECTION"
    }
    {
        name: "test1",
        lbmethod: "LEASTCONNECTION"
    }
}
```

- `Using REST APIs through SDKs`

  To retrieve the properties of a resource, you retrieve the resource object from the Citrix ADC appliance. Once the object is retrieved, you can extract the required properties of the resource locally, without further network traffic.

The following sample code retrieves the details of a load balancing virtual server.

`Java - Sample code to get details of resource`

```
//Retrieve the resource object from the Citrix ADC


new_lbvserver_obj = lbvserver.get(ns_session,"MyFirstLbVServer");


//Extract the properties of the resource from the object locally
```

```
System.out.println(new_lbvserver_obj.get_name());

System.out.println(new_lbvserver_obj.get_servicetype());
```

`.NET - Sample code to get details of resource`

```
//Retrieve the resource object from the Citrix ADC

new_lbvserver_obj = lbvserver.get(ns_session,"MyFirstLbVServer");

//Extract the properties of the resource from the object locally

Console.WriteLine(new_lbvserver_obj.name);

Console.WriteLine(new_lbvserver_obj.servicetype);
```

`Python - Sample code to get details of resource`

```
# Retrieve the resource object from the CItrix ADC

new_lbvserver_obj = lbvserver.get(ns_session,"MyFirstLbVServer")

# Extract the properties of the resource from the object locally

print(new_lbvserver_obj.name)
```

```
print(new_lbvserver_obj.servicetype)
```

Filtering Results

This topic covers retrieving filtered information of a resource by using REST APIs through SDKs.

- `Using REST APIs through SDKs`

  You can also retrieve resources by specifying a filter on the value of their properties by using the com.citrix.netscaler.nitro.util.filtervalue class.

For example, you can retrieve all the load balancing virtual servers that have their port set to 80 and servicetype to HTTP.

`Java - Sample code to get filtered results`

```
filtervalue[] filter = new filtervalue[2];

filter[0] = new filtervalue("port","80");

filter[1] = new filtervalue("servicetype","HTTP");

lbvserver[] result = lbvserver.get_filtered(ns_session,filter);
```

`.NET - Sample code to get filtered results`

```
filtervalue[] filter = new filtervalue[2];

filter[0] = new filtervalue("port","80");

filter[1] = new filtervalue("servicetype","HTTP");

lbvserver[] result = lbvserver.get_filtered(ns_session,filter);
```

`Python - Sample code to get filtered results`

```
filter_params = []



      filter_params = [ filtervalue() for _ in range(2)]
```

```
filter_params[0] = filtervalue("servicetype","HTTP")

filter_params[1] = filtervalue("port","80")

result = lbvserver.get_filtered(ns_session1, filter_params)
```

Retrieving Statistics of Citrix ADC Resources

The Citrix ADC appliance collects statistics about the usage of its features and the corresponding resources. NITRO can retrieve these statistics. Not all Citrix ADC features and resources have statistic objects associated with them.

- `Using REST APIs through HTTP`

  To get statistics of a feature, the URL format must be: http://<Citrix-ADC-IP-address(NSIP)>/nitro/v1/stat/\<feature_name\>.

To get statistics of a resource, the URL format must be: http://<Citrix-ADC-IP-address(NSIP)>/nitro/v1/stat/\<resource_type\>/\<resource_name\>.

To get statistics of the services and service groups that are bound to a load balancing virtual server, the URL format must be: http://<Citrix-ADC-IP-address(NSIP)>/nitro/v1/stat/lbvserver/\<name\>?statbindings=yes*.

- `Request`

  `HTTP Method:` GET

`URL:` http://<Citrix-ADC-IP-address(NSIP)>/nitro/v1/stat/lbvserver/MyFirstLbVServer

`Request Headers:`

Cookie:NITRO_AUTH_TOKEN=\<tokenvalue\>

Accept:application/json

- `Response`

  `HTTP Status Code on Success:` 200 OK

`HTTP Status Code on Failure:`

4xx <string> (for general HTTP errors) or 5xx <string> (for Citrix-ADC-specific errors). The response payload provides details of the error.

`Response Payload:`

```
{

    "lbvserver":

    [

        {

            "name":"MyFirstLbVServer",

            "establishedconn":0,

            "vslbhealth":0,

            "primaryipaddress":"0.0.0.0",

            ...
```

```
        }

    ]

}
```

To get statistics of the bound entities, use statbindings=yes. For example, to get the statistics of the services that are bound to a load balancing virtual server named MyFirstLbVServer.

- `Request`

  `HTTP Method:` GET

`URL:` http://<Citrix-ADC-IP-address(NSIP)>/nitro/v1/stat/lbvserver/MyFirstLbVServer?statbindings=yes

`Request Headers:`

Cookie:NITRO_AUTH_TOKEN=\<tokenvalue\>

Accept:application/json

- `Response`

  `HTTP Status code on success:` 200 OK

`HTTP Status code on failure:`

4xx <string> (for general HTTP errors) or 5xx <string> (for Citrix-ADC-specific errors). The response payload provides details of the error.

`Response Header:`

Content-Type:application/json

`Response Payload:`

```
{

"lbvserver": [{

    "name": "MyFirstLbVServer",

    "sortorder": "descending",

    "vsvrsurgecount": "0",

    "establishedconn": "0",

    ...

    "service": [{

        "name": "s1",

        "throughput": "0",

        "throughputrate": 0,
```

```
        "avgsvrttfb": "0",

        "primaryipaddress": "1.2.3.5",

        "primaryport": 80,

        "servicetype": "HTTP",

        "state": "DOWN",

            "totalrequests": "0",

            "requestsrate": 0,

            ...

            }]
    }]

}
```

- `Using REST APIs through SDKs`

The Citrix ADC appliance collects statistics about the usage of its features and the corresponding resources. You can retrieve these statistics by using NITRO API. The statistics APIs are available in different packages from the configuration APIs.

For example, the API to retrieve statistics of the load balancing virtual server are available in com.citrix.netscaler.nitro.resource.stat.lb.

`Note.`

- For the python SDK, the package path is of the form nssrc.com.citrix.netscaler.....
- Not all Citrix ADC features and resources have statistic objects associated with them.

The following sample code retrieves the statistics of a load balancing virtual server and displays some of the statistics returned.

`Java - Sample code to get feature statistics`

```
lbvserver_stats stats =
lbvserver_stats.get(ns_session,"MyFirstLbVServer");



System.out.println(stats.get_curclntconnections());



System.out.println(stats.get_deferredreqrate());
```

`.NET - Sample code to get feature statistics`

```
lbvserver_stats stats =
lbvserver_stats.get(ns_session,"MyFirstLbVServer");



Console.WriteLine(stats.curclntconnections);



Console.WriteLine(stats.deferredreqrate);
```

`Python - Sample code to get feature statistics`

```
stats = lbvserver_stats.get(ns_session,"MyFirstLbVServer")



print(stats.curclntconnections)



print(stats.deferredreqrate)
```

Retrieving Statistics of Citrix ADC Resources

The Citrix ADC appliance collects statistics about the usage of its features and the corresponding resources. NITRO can retrieve these statistics. Not all Citrix ADC features and resources have statistic objects associated with them.

- `Using REST APIs through HTTP`

  To get statistics of a feature, the URL format must be: http://<Citrix-ADC-IP-address(NSIP)>/nitro/v1/stat/\<feature_name\>.

To get statistics of a resource, the URL format must be: http://<Citrix-ADC-IP-address(NSIP)>/nitro/v1/stat/\<resource_type\>/\<resource_name\>.

To get statistics of the services and service groups that are bound to a load balancing virtual server, the URL format must be: http://<Citrix-ADC-IP-address(NSIP)>/nitro/v1/stat/lbvserver/\<name\>?statbindings=yes*.

- `Request`

  `HTTP Method:` GET

`URL:` http://<Citrix-ADC-IP-address(NSIP)>/nitro/v1/stat/lbvserver/MyFirstLbVServer

`Request Headers:`

Cookie:NITRO_AUTH_TOKEN=\<tokenvalue\>

Accept:application/json

- `Response`

  `HTTP Status Code on Success:` 200 OK

`HTTP Status Code on Failure:`

4xx <string> (for general HTTP errors) or 5xx <string> (for Citrix-ADC-specific errors). The response payload provides details of the error.

`Response Payload:`

```
{

    "lbvserver":

    [

        {

            "name":"MyFirstLbVServer",

            "establishedconn":0,

            "vslbhealth":0,

            "primaryipaddress":"0.0.0.0",

            ...
```

```
        }


    ]


}
```

To get statistics of the bound entities, use statbindings=yes. For example, to get the statistics of the services that are bound to a load balancing virtual server named MyFirstLbVServer.

- `Request`

  `HTTP Method:` GET

`URL:` http://<Citrix-ADC-IP-address(NSIP)>/nitro/v1/stat/lbvserver/MyFirstLbVServer?statbindings=yes

`Request Headers:`

Cookie:NITRO_AUTH_TOKEN=\<tokenvalue\>

Accept:application/json

- `Response`

  `HTTP Status code on success:` 200 OK

`HTTP Status code on failure:`

4xx <string> (for general HTTP errors) or 5xx <string> (for Citrix-ADC-specific errors). The response payload provides details of the error.

`Response Header:`

Content-Type:application/json

`Response Payload:`

```
{

"lbvserver": [{

    "name": "MyFirstLbVServer",

    "sortorder": "descending",

    "vsvrsurgecount": "0",

    "establishedconn": "0",

    ...

    "service": [{

        "name": "s1",

        "throughput": "0",

        "throughputrate": 0,
```

```
        "avgsvrttfb": "0",

        "primaryipaddress": "1.2.3.5",

        "primaryport": 80,

        "servicetype": "HTTP",

        "state": "DOWN",

            "totalrequests": "0",

            "requestsrate": 0,

            ...

            }]
    }]

}
```

- `Using REST APIs through SDKs`

The Citrix ADC appliance collects statistics about the usage of its features and the corresponding resources. You can retrieve these statistics by using NITRO API. The statistics APIs are available in different packages from the configuration APIs.

For example, the API to retrieve statistics of the load balancing virtual server are available in com.citrix.netscaler.nitro.resource.stat.lb.

`Note:`

- For the python SDK, the package path is of the form nssrc.com.citrix.netscaler.....
- Not all Citrix ADC features and resources have statistic objects associated with them.

The following sample code retrieves the statistics of a load balancing virtual server and displays some of the statistics returned.

`Java - Sample code to get feature statistics`

```
lbvserver_stats stats =
lbvserver_stats.get(ns_session,"MyFirstLbVServer");



System.out.println(stats.get_curclntconnections());



System.out.println(stats.get_deferredreqrate());
```

`.NET - Sample code to get feature statistics`

```
lbvserver_stats stats =
lbvserver_stats.get(ns_session,"MyFirstLbVServer");



Console.WriteLine(stats.curclntconnections);



Console.WriteLine(stats.deferredreqrate);
```

`Python - Sample code to get feature statistics`

```
stats = lbvserver_stats.get(ns_session,"MyFirstLbVServer")



print(stats.curclntconnections)



print(stats.deferredreqrate)
```

Updating a Citrix ADC Resource

You can modify the properties of a resource after creating it.

Some properties in some Citrix ADC resources are not allowed to be modified after creation. The port number or the service type (protocol) of a load balancing virtual server or a service, are examples of such properties. Even though the update method appears to succeed, these properties retain their original values on the appliance.

- `Using REST APIs through HTTP`

  To update the details of an existing resource on the Citrix ADC appliance, specify the name of the resource in the URL, and in the request payload,within the specific resource object, specify the name and the updated details of the resource.

For example, to change the load balancing method to ROUNDROBIN and update the comment property for a load balancing virtual server named MyFirstLbVServer:

- `Request`

  `HTTP Method:` PUT

`URL:` http://<Citrix-ADC-IP-address(NSIP)>/nitro/v1/config/lbvserver/MyFirstLbVServer

`Request Headers:`

Cookie:NITRO_AUTH_TOKEN=<tokenvalue>

Content-Type:application/json

`Request Payload:`

```
{

    "lbvserver":

    {

        "name":"MyFirstLbVServer",

        "lbmethod":"ROUNDROBIN",

        "comment":"Updated comments"

    }

}
```

- `Response`

  `HTTP Status Code on Success:` 200 OK

`HTTP Status Code on Failure:`

4xx <string> (for general HTTP errors) or 5xx <string> (for Citrix-ADC-specific errors). The response payload provides details of the error.

- `Using REST APIs through SDKs`

  To update the properties of a resource, instantiate the resource class, specify the name of the resource to be updated, configure the resource by updating its properties locally, and then upload the updated resource instance to the Citrix ADC appliance.

The following sample code updates the service type and load balancing method of a load balancing virtual server.

`Java - Sample code to update a Citrix ADC resource`

```
//Create an instance of the lbvserver class



lbvserver update_lb = new lbvserver();
```

```
//Specify the name of the lbvserver to be updated

update_lb.set_name("MyFirstLbVServer");

//Specify the updated service type and lb method

update_lb.set_servicetype("https");
update_lb.set_lbmethod("LEASTRESPONSETIME");

//Upload the resource to Citrix ADC

lbvserver.update(ns_session,update_lb);
```

`.NET - Sample code to update a Citrix ADC resource`

```
//Create an instance of the lbvserver class

lbvserver update_lb = new lbvserver();

//Specify the name of the lbvserver to be updated

update_lb.name = "MyFirstLbVServer";
```

```
//Specify the updated service type and lb method



update_lb.servicetype = "https";

update_lb.lbmethod = "LEASTRESPONSETIME";



//Upload the resource to Citrix ADC



lbvserver.update(ns_session, update_lb);
```

`Python - Sample code to update a Citrix ADC resource`

```
# Create an instance of the lbvserver class



update_lb = lbvserver()



# Specify the name of the lbvserver to be updated



update_lb.name = "MyFirstLbVServer"



# Specify the updated service type and lb method



update_lb.servicetype = "https"
```

```
update_lb.lbmethod = "LEASTRESPONSETIME"



# Upload the resource to the CItrix ADC



lbvserver.update(ns_session, update_lb)
```

Binding Citrix ADC Resources

Citrix ADC resources form relationships with each other through the process of binding. This is how services are associated with a load balancing virtual server, or how policies are bound to a load balancing virtual server. Each binding relationship is represented by its own object.

A binding resource has properties representing the name of each Citrix ADC resource in the binding relationship. It can also have other properties related to that relationship (for example, the weight of the binding between an lbvserver resource and a service resource).

- `Using REST APIs through HTTP`

  To bind one Citrix ADC resource to another, you must instantiate the appropriate binding class (for example, to bind a service to a load balancing virtual server, you must instantiate the lbvserver_service_binding class) and add it to the Citrix ADC configuration (by using the static add() method on this class).

To unbind a resource, use the DELETE method and specify an "args" query string parameter in the URL that contains the attribute name and value in the relationship resource that designates the secondary resource.

The following example binds a service named svc_prod to a load balancing virtual server named MyFirstLbVServer and specify a weight for the binding.

- `Request`

  `HTTP Method:` POST

`URL:` http://<Citrix-ADC-ip-address(NSIP)\>/nitro/v1/config/lbvserver_service_binding

`Request Headers:` Cookie:NITRO_AUTH_TOKEN=<tokenvalue> Content-Type:application/json

`Request Payload:`

```
{

"lbvserver_service_binding":

    {

    "servicename":"svc_prod",

    "weight":"20",

    "name":"MyFirstLbVServer"

    }

}
```

- `Response`

  `HTTP Status Code on Success:` 201 Created

`HTTP Status Code on Failure:` 4xx \<string \> (for general HTTP errors) or 5xx \<string \> (for Citrix-ADC-specific errors). The response payload provides details of the error.

The following example binds a policy to a policy label.

- `Request`

  `HTTP Method:` POST

`URL:` http://<Citrix-ADC-ip-address(NSIP)\>/nitro/v1/config/authenticationpolicylabel_authenticationpolicy_binding

`Request Headers:`

Cookie:NITRO_AUTH_TOKEN=<tokenvalue>

Content-Type:application/json

`Request Payload:`

```
{

"authenticationpolicylabel_authenticationpolicy_binding":

    {

    "policyname":"p1",

    "priority":"100",

    "gotopriorityexpression":"END",

    "labelname":"pl1"

    }

}
```

- `Response`

  `HTTP Status Code on Success:` 201 Created

`HTTP Status Code on Failure:`

4xx <string> (for general HTTP errors) or 5xx <string> (for Citrix-ADC-specific errors). The response payload provides details of the error.

The following example unbinds the service svc_prod from the load balancing virtual server MyFirstLbVServer.

- `Request`

  `HTTP Method:` DELETE

`URL:` http://<Citrix-ADC-IP-address(NSIP)>/nitro/v1/config/lbvserver_service_binding/MyFirstLbVServer?args=servicename:svc_prod

`Request Header:`

Cookie:NITRO_AUTH_TOKEN=\<tokenvalue\>

- `Response`

  `HTTP Status Code on Success:` 200 OK

`HTTP Status Code on Failure:`

4xx <string> (for general HTTP errors) or 5xx <string> (for Citrix-ADC-specific errors). The response payload provides details of the error.

- `Using REST APIs through SDKs`

  To bind one Citrix ADC resource to another, you must instantiate the appropriate binding class (for example, to bind a service to a load balancing virtual server, you must instantiate the lbvserver_service_binding class) and add it to the Citrix ADC configuration (by using the static add() method on this class).

To unbind a resource from another, invoke the delete() method from the resource binding class, by passing the name of the two resources.

The following sample code binds a service to a load balancing virtual server, by specifying a certain weight for the binding.

`Java - Sample code for binding`

```
lbvserver_service_binding bindObj = new lbvserver_service_binding();

bindObj.set_name("MyFirstLbVServer");

bindObj.set_servicename("svc_prod");

bindObj.set_weight(20);

lbvserver_service_binding.add(ns_session,bindObj);
```

`.NET - Sample code for binding`

```
lbvserver_service_binding bindObj = new lbvserver_service_binding();

bindObj.name = "MyFirstLbVServer";

bindObj.servicename = "svc_prod";

bindObj.weight = 20;

lbvserver_service_binding.add(ns_session,bindObj);
```

`Python - Sample code for binding`

```
bindObj = lbvserver_service_binding()

bindObj.name = "MyFirstLbVServer"

bindObj.servicename = "svc_prod"

bindObj.weight = 20

lbvserver_service_binding.add(ns_session, bindObj)
```

The following code sample unbinds a service from a server.

`Java - Sample Code for unbinding`

```
lbvserver_service_binding bindObj = new lbvserver_service_binding();

bindObj.set_name("MyFirstLbVServer");

bindObj.set_servicename("svc_prod");

lbvserver_service_binding.delete(ns_session,bindObj);
```

`.NET - Sample code for unbinding`

```
lbvserver_service_binding bindObj = new lbvserver_service_binding();

bindObj.name("MyFirstLbVServer");

bindObj.servicename("svc_prod");

lbvserver_service_binding.delete(ns_session,bindObj);
```

`Python - Sample code for unbinding`

```
bindObj = lbvserver_service_binding()

bindObj.name = "MyFirstLbVServer"

bindObj.servicename = "svc_prod"
```

```
lbvserver_service_binding.delete(ns_session, bindObj)
```

Globally Binding Citrix ADC Resources

Some Citrix ADC resources can be bound globally to affect the whole system. For example, a compression policy can be bound to an load balancing virtual server, in which case the policy affects only the traffic on that load balancing virtual server. However, if bound globally, it can affect any traffic on the appliance, regardless of which virtual servers handle the traffic.

The names of NITRO resources that can be used to bind resources globally have the pattern *\<featurename \>global_\<resourcetype \>_binding*. For example, the object *aaaglobal_aaapreauthenticationpolicy_binding* is used to bind preauthentication policies globally.

- `Using REST APIs through HTTP`

  The following example binds the policy named preautpol1 globally at priority 200.

- `Request`

  `HTTP Method:` POST

`URL:`

http://<Citrix-ADC-ip-address(NSIP)\>/nitro/v1/config/aaaglobal_aaapreauthenticationpolicy_binding/preautpol1

`Request Headers:`

Cookie:NITRO_AUTH_TOKEN=<tokenvalue>

Content-Type:application/json

`Request Payload:`

```
{

"aaaglobal_aaapreauthenticationpolicy_binding":

    {

    "policy":"preautpol1",
```

```
    "priority":"200"

    }

}
```

- `Response`

  `HTTP Status Code on Success:` 200 OK

`HTTP Status Code on Failure:`

4xx <string> (for general HTTP errors) or 5xx <string> (for Citrix-ADC-specific errors). The response payload provides details of the error.

The following example unbinds the policy named preautpol1.

- `Request`

  `HTTP Method:` DELETE

`URL:`

http://<Citrix-ADC-ip-address(NSIP)\>/nitro/v1/config/aaaglobal_aaapreauthenticationpolicy_binding?args=policy:preautpol1

`Request Header:`

Cookie:NITRO_AUTH_TOKEN=\<tokenvalue\>

- `Response`

  `HTTP Status Code on Success:` 200 OK

`HTTP Status Code on Failure:`

4xx <string> (for general HTTP errors) or 5xx <string> (for Citrix-ADC-specific errors). The response payload provides details of the error.

- `Using REST APIs through SDKs`

  The following sample code creates a preauthentication action and a preauthentication policy that uses that action, and then binds the policy globally at priority 200.

Java - Sample code

```
aaapreauthenticationaction preauth_act1;

aaapreauthenticationpolicy preauth_pol1;

aaaglobal_aaapreauthenticationpolicy_binding glob_binding;

preauth_act1 = new aaapreauthenticationaction();

preauth_act1.set_name("preauth_act1");

preauth_act1.set_preauthenticationaction("ALLOW");

aaapreauthenticationaction.add(ns_session,preauth_act1);

preauth_pol1 = new aaapreauthenticationpolicy();

preauth_pol1.set_name("preauth_pol1");

preauth_pol1.set_rule("CLIENT.APPLICATION.PROCESS(antivirus.exe) EXISTS");

preauth_pol1.set_reqaction("preauth_act1");
```

```
aaapreauthenticationpolicy.add(ns_session,preauth_pol1);

 glob_binding = new aaaglobal_aaapreauthenticationpolicy_binding();

glob_binding.set_policy("preauth_pol1");

glob_binding.set_priority(200);

aaaglobal_aaapreauthenticationpolicy_binding.add(ns_session,glob_binding);
```

`.NET - Sample code`

```
aaapreauthenticationaction preauth_act1;

aaapreauthenticationpolicy preauth_pol1;

aaaglobal_aaapreauthenticationpolicy_binding glob_binding;

preauth_act1 = new aaapreauthenticationaction();

preauth_act1.name = "preauth_act1";
```

```
preauth_act1.preauthenticationaction = "ALLOW";

aaapreauthenticationaction.add(ns_session, preauth_act1);

preauth_pol1 = new aaapreauthenticationpolicy();

preauth_pol1.name = "preauth_pol1";

preauth_pol1.rule = "CLIENT.APPLICATION.PROCESS(antivirus.exe) EXISTS";

preauth_pol1.reqaction = "preauth_act1";

aaapreauthenticationpolicy.add(ns_session, preauth_pol1);

glob_binding = new aaaglobal_aaapreauthenticationpolicy_binding();

glob_binding.policy = "preauth_pol1";

glob_binding.priority = 200;

aaaglobal_aaapreauthenticationpolicy_binding.add(ns_session,glob_binding);
```

Python - Sample code

```
preauth_act1 = aaapreauthenticationaction()

preauth_act1.name = "preauth_act1"

preauth_act1.preauthenticationaction = "ALLOW"

aaapreauthenticationaction.add(ns_session, preauth_act1)

preauth_pol1 = aaapreauthenticationpolicy()

preauth_pol1.name = "preauth_pol1"

preauth_pol1.rule = "CLIENT.APPLICATION.PROCESS(antivirus.exe) EXISTS"

preauth_pol1.reqaction = "preauth_act1"

aaapreauthenticationpolicy.add(ns_session, preauth_pol1)

glob_binding = aaaglobal_aaapreauthenticationpolicy_binding()

glob_binding.policy = "preauth_pol1"
```

```
glob_binding.priority = 200


aaaglobal_aaapreauthenticationpolicy_binding.add(ns_session, glob_binding)
```

Deleting a Citrix ADC Resource

The usage of the delete operation depends on the unique identifiers (UIDs) of the resource being deleted.

Deleting Resource with Single UID. To delete a Citrix ADC resource that can be identified by a single identifier, specify the resource name. Deleting Resource with Multiple UIDs. To delete a Citrix ADC resource that is identified using multiple identifiers, use the "args" query parameter to specify the unique attributes along with their values.

- `Using REST APIs through HTTP`

  The following example deletes a load balancing virtual server named MyFirstLbVServer.

- `Request`

  `HTTP Method:` DELETE

`URL:` http://<Citrix-ADC-IP-address(NSIP)>/nitro/v1/config/lbvserver/MyFirstLbVServer

`Request Header:` Cookie:NITRO_AUTH_TOKEN=\<tokenvalue\>

- `Response`

  `HTTP Status Code on Success:` 200 OK

`HTTP Status Code on Failure:`

4xx <string> (for general HTTP errors) or 5xx <string> (for Citrix-ADC-specific errors). The response payload provides details of the error.

The following example deletes a resource with multiple UIDs. Consider a SNIP (10.102.29.71) that belongs to two traffic domains (TDs) 123 and 110. To delete the SNIP from one of the traffic domains, specify the IP address and the relevant TD in the URL as follows:

- `Request`

  `HTTP Method:` DELETE

`URL:`

http://<Citrix-ADC-IP-address(NSIP)>/nitro/v1/config/nsip?args=ipaddress:10.102.29.71,td:123

`Request Header:` Cookie:NITRO_AUTH_TOKEN=\<tokenvalue\>

- `Response`

  `HTTP Status Code on Success:` 200 OK

`HTTP Status Code on Failure:`

4xx <string> (for general HTTP errors) or 5xx <string> (for Citrix-ADC-specific errors). The response payload provides details of the error.

- `Using REST APIs through SDKs`

  To delete an existing resource, invoke the static method delete() on the resource class, by passing the name of the resource.

The following sample code deletes a load balancing virtual server with name MyFirstLbVServer.

`Java - Sample code to delete a Citrix ADC resource`

```
lbvserver remove_lb = new lbvserver();

remove_lb.set_name("MyFirstLbVServer");

lbvserver.delete(ns_session, remove_lb);
```

`.NET - Sample code to delete a Citrix ADC resource`

```
lbvserver remove_lb = new lbvserver();

remove_lb.name("MyFirstLbVServer");

lbvserver.delete(ns_session, remove_lb);
```

`Python - Sample code to delete a Citrix ADC resource`

```
remove_lb = lbvserver()

remove_lb.name = "MyFirstLbVServer"

lbvserver.delete(ns_session, remove_lb)
```

Performing Bulk Operations

You can create, retrieve, update, and delete multiple resources simultaneously and thus minimize network traffic. For example, you can add multiple load balancing virtual servers in the same operation.

To account for the failure of some operations within the bulk operation, NITRO allows you to configure one of the following behaviors while establishing a connection with the appliance.

- `Exit`. When the first error is encountered, the execution stops. The commands that were executed before the error are committed.
- `Rollback`. When the first error is encountered, the execution stops. The commands that were executed before the error are rolled back. Rollback is only supported for add and bind commands.
- `Continue`. All the commands in the list are executed even if some commands fail.
- `Using REST APIs through HTTP`

  To perform a bulk operation, specify the required parameters in the same request payload. You must specify the behavior of the bulk operation in the request header using the X-NITRO-ONERROR parameter.

The following example adds two load balancing virtual servers in one operation. The operation continues even if one of the add operation fails.

- `Request`

  `HTTP Method:` POST

`URL:` http://<Citrix-ADC-IP-address(NSIP)>/nitro/v1/config/lbvserver

`Request Headers:`

Cookie:NITRO_AUTH_TOKEN=<tokenvalue>

Content-Type:application/json

`Request Payload:`

```
{

    "lbvserver":

    [

        {

        "name":"new_lbvserver1",

        "servicetype":"http"

        },



        {

        "name":"new_lbvserver2",

        "servicetype":"http"

        }

    ]

}
```

- `Response`

  `HTTP Status Code on Success:` 201 Created for the add operation and 200 OK for the update operation.

`HTTP Status Code on Failure:` 207 Multi Status with error details in the response payload.

The following example enables multiple load balancing virtual servers in the same operation.

- `Request`

  `HTTP Method:` POST

`URL:` http://<Citrix-ADC-IP-address(NSIP)>/nitro/v1/config/lbvserver?action=enable

`Request Headers:`

Cookie:NITRO_AUTH_TOKEN=\<tokenvalue\>

Content-Type:application/json

`Request Payload:`

```
{
            "lbvserver":
    [
        {
            "name":"v1",
        },


        {
            "name":"v2",
        }
    ]
}
```

- `Response`

  `HTTP Status Code on Success:` 201 Created for the add operation and 200 OK for the update operation.

`HTTP Status Code on Failure:` 207 Multi Status with error details in the response payload.

- `Using REST APIs through SDKs`

To perform a bulk operation, you instantiate an array of the resource class, configure the properties of all the instances locally, and then upload all the instances to the Citrix ADC with one command.

The following sample code specifies bulk operation behavior.

`Java - Sample code to specify bulk operation behavior`

```
nitro_service ns_session = new nitro_service("10.102.29.60","http");

ns_session.set_onerror(OnerrorEnum.CONTINUE);

ns_session.login("admin","verysecret");
```

`.NET - Sample code to specify bulk operation behavior`

```
nitro_service ns_session = new nitro_service("10.102.29.60","http");

ns_session.onerror = OnerrorEnum.CONTINUE;

ns_session.login("admin","verysecret");
```

`Python - Sample code to specify bulk operation behavior`

```
ns_session = nitro_service("10.102.29.60","http")

ns_session.onerror = OnerrorEnum.CONTINUE

ns_session.login("admin","verysecret")
```

The following sample code creates two load balancing virtual servers.

`Java - Sample code for bulk creation`

```
//Create an array of lbvserver instances



lbvserver[] lbs = new lbvserver[2];
```

```
//Specify properties of the first lbvserver


lbs[0] = new lbvserver();

lbs[0].set_name("lbvserv1");

lbs[0].set_servicetype("http");

lbs[0].set_ipv46("10.70.136.5");

lbs[0].set_port(80);


//Specify properties of the second lbvserver


lbs[1] = new lbvserver();

lbs[1].set_name("lbvserv2");

lbs[1].set_servicetype("https");

lbs[1].set_ipv46("10.70.136.5");

lbs[1].set_port(443);


//Upload the properties of the two lbvservers to the Citrix ADC


lbvserver.add(ns_session,lbs);
```

`.NET - Sample code for bulk creation`

```
//Create an array of lbvserver instances

lbvserver[] lbs = new lbvserver[2];



//Specify details of first lbvserver



lbs[0] = new lbvserver();

lbs[0].name = "lbvserv1";

lbs[0].servicetype = "http";

lbs[0].ipv46 = "10.70.136.5";

lbs[0].port = 80;



//Specify details of second lbvserver



lbs[1] = new lbvserver();

lbs[1].name = "lbvserv2";

lbs[1].servicetype = "https";

lbs[1].ipv46 = "10.70.136.5";

lbs[1].port = 443;



//upload the details of the lbvservers to the NITRO server
```

```
lbvserver.add(ns_session,lbs);
```

`Python - Sample code for bulk creation`

```
# Create an array of lbvserver instances

lbs = lbvserver[2]

# Specify properties of the first lbvserver

lbs[0] = lbvserver()
lbs[0].name = "lbvserv1"
lbs[0].servicetype = "http"
lbs[0].ipv46 = "10.70.136.5"
lbs[0].port = 80

# Specify properties of the second lbvserver

lbs[1] = lbvserver()
lbs[1].name = "lbvserv2"
lbs[1].servicetype = "https"
lbs[1].ipv46 = "10.70.136.5"
```

```
lbs[1].port = 443



# Upload the properties of the two lbvservers to the CItrix ADC



lbvserver.add(ns_session, lbs)
```

Getting the Count of Citrix ADC Resources

This topic covers getting the count of a type of Citrix ADC resource present in a Citrix ADC appliance by using REST APIs through HTTP.

- `Using REST APIs through HTTP`

  To get a count of a specific resource type, in the URL specify the count query parameter as "yes".

For example, to get a count of all the load balancing virtual servers.

- `Request`

  `HTTP Method:` GET

`URL:` http://<Citrix-ADC-IP-address(NSIP)>/nitro/v1/config/lbvserver?count=yes

`Request Headers:`

Cookie:NITRO_AUTH_TOKEN=<tokenvalue>

Accept:application/json

- `Response`

  `HTTP Status Code on Success:` 200 OK

`HTTP Status Code on Failure:`

4xx <string> (for general HTTP errors) or 5xx <string> (for Citrix-ADC-specific errors). The response payload provides details of the error.

`Response Header:`

Content-Type:application/json

`Response Payload:`

```
{
    "lbvserver":
    [
        {
            "__count": 4
        }
    ]
}
```

Renaming a Citrix ADC Resource

This topic covers renaming a Citrix ADC resource by using REST APIs through HTTP.

- `Using REST APIs through HTTP`

  To change the name of an existing resource, specify the action as "rename" in the URL query string, and in the request payload, specify the existing name and the new name.

For example, to change the name of a load balancing virtual server from MyFirstLbVServer to MyServer:

- `Request`

  `HTTP Method:` POST

`URL:` http://<Citrix-ADC-ip-address(NSIP)\>/nitro/v1/config/lbvserver?action=rename

`Request Headers:`

Cookie:NITRO_AUTH_TOKEN=<tokenvalue>

Content-Type:application/json

`Request Payload:`

```
{

    "lbvserver":

    {

        "name":"MyFirstLbVServer",

        "newname":"MyServer"

    }

}
```

- `Response`

  `HTTP Status Code on Success:` 200 OK

`HTTP Status Code on Failure:`

4xx <string> (for general HTTP errors) or 5xx <string> (for Citrix-ADC-specific errors). The response payload provides details of the error.

Performing File Operations

Citrix ADC operations such as configuring SSL certificates requires the input files to be available locally on the Citrix ADC appliance. NITRO allows you to perform file operations such as uploading files, retrieving files, retrieving file content, and deleting files of types: txt, cert, req, xml, lic, and key.

- `Notes`
  - File size must be less than or equal to 2 MB.
- Use the "BASE64" value for the fileencoding attribute in the request payload. This is the only valid encoding currently supported.
- The filelocation path must be URL encoded. For example, if the path is /nsconfig/ssl, encode the / and use the file location as %2Fnsconfig%2Fssl.

- When uploading a file, make sure that each directory of the file path has the 755 (read, write, execute) permission. For example, to upload a file to the "/nsconfig/ssl.html" directory, the following directories must have the 755 permission: flash (because the "/nsconfig" folder is actually a link to "/flash/nsconfig.html" directory)
  - nsconfig
  - ssl

Uploading a File

To upload a file to the Citrix ADC, specify a name for the file, the location where the file must be created on the Citrix ADC, and the content of the file.

- `Using REST APIs through HTTP`

  For example, to upload a file named cert1.crt in the /nsconfig/ssl/ directory:

- `Request`

  `HTTP Method:` POST

`URL:` http://<Citrix-ADC-IP-address(NSIP)>/nitro/v1/config/systemfile

`Request Headers:`

Cookie:NITRO_AUTH_TOKEN=<tokenvalue>

Content-Type:application/json

`Request Payload:`

```
{

        "systemfile":

        {

            "filename": "cert1.crt",

            "filelocation": "/nsconfig/ssl.html",

            "filecontent":"VGhpcyBpcyBteSBmaWxl",

            "fileencoding": "BASE64"
```

```
        }

}
```

- `Response`

  `HTTP Status Code on Success:` 200 OK

`HTTP Status Code on Failure:`

4xx <string> (for general HTTP errors) or 5xx <string> (for Citrix-ADC-specific errors). The response payload provides details of the error.

Retrieving the Files

To retrieve the files from a specific Citrix ADC directory, specify the directory path in the URL.

- `Using REST APIs through HTTP`

  For example, to retrieve the files from the /nsconfig/ssl directory.

- `Request`

  `HTTP Method:` GET

`URL:`

http://<Citrix-ADC-IP-address(NSIP)>/nitro/v1/config/systemfile?args=filelocation:%2Fnsconfig%2Fssl

`Request Header:`

Cookie:NITRO_AUTH_TOKEN=\<tokenvalue\>

Accept:application/json

- `Response`

  `HTTP Status Code on Success:` 200 OK

`HTTP Status Code on Failure:`

4xx <string> (for general HTTP errors) or 5xx <string> (for Citrix-ADC-specific errors). The response payload provides details of the error.

`Response Header:`

Content-Type:application/json

`Response Payload:`

```
{

    "systemfile":

    [

            "filename": "ns-root.key",

            "filelocation": "/nsconfig/ssl",

            "fileaccesstime": "Tue Jan 14 19:27:01 2014",

            "filemodifiedtime": "Tue Nov  5 17:16:00 2013"

        },

        {

        {

            "filename": "ns-root.req",

            "filelocation": "/nsconfig/ssl",

            "fileaccesstime": "Tue Jan 14 19:27:01 2014",

            "filemodifiedtime": "Tue Nov  5 17:16:00 2013"

        }

    ]

}
```

Retrieving Contents of a Specific File

To retrieve the contents of a file, specify the filename and its directory path in the URL.

- `Using REST APIs through HTTP`

  For example, to retrieve the contents of the ns-root.key file from the /nsconfig/ssl directory.

- `Request`

  `HTTP Method:` GET

`URL:` http://<Citrix-ADC-IP-address(NSIP)>/nitro/v1/config/systemfile/ns-root.key?args=filelocation:%2Fnsconfig%2Fssl

`Request Header:`

Cookie:NITRO_AUTH_TOKEN=\<tokenvalue\>

Accept:application/json

- `Response`

  `HTTP Status Code on Success:`

200 OK

`HTTP Status Code on Failure:`

4xx <string> (for general HTTP errors) or 5xx <string> (for Citrix ADC specific errors). The response payload provides details of the error.

`Response Header:`

Content-Type:application/json

`Response Payload:`

```
{

    "systemfile":

    [

        {

            "filename": "ns-root.key",

            "filelocation": "/nsconfig/ssl",
```

```
            "filecontent": "LS0tLS1CRUdJTiBSU0EgUFJJVkFU0tLQo=",
            "fileencoding": "BASE64",
            "fileaccesstime": "Tue Jan 14 19:27:01 2014",
            "filemodifiedtime": "Tue Nov  5 17:16:00 2013"
        }
    ]
}
```


Deleting a File

To delete a file from the Citrix ADC appliance, specify the filename and the directory path in the URL.

- `Using REST APIs through HTTP`

  For example, to delete the ns-root.key file from the /nsconfig/ssl directory.

`Request:`

`HTTP Method:` DELETE

`URL:` https://<Citrix-ADC-IP-address(NSIP)>/nitro/v1/config/systemfile/ns-root.key?args=filelocation:%2Fnsconfig%2Fssl

`Request Header:`

Cookie:NITRO_AUTH_TOKEN=\<tokenvalue\>

- `Response`

  `HTTP Status Code on Success:` 200 OK

`HTTP Status Code on Failure:`

4xx <string> (for general HTTP errors) or 5xx <string> (for Citrix-ADC-specific errors). The response payload provides details of the error.

Use Cases and Samples

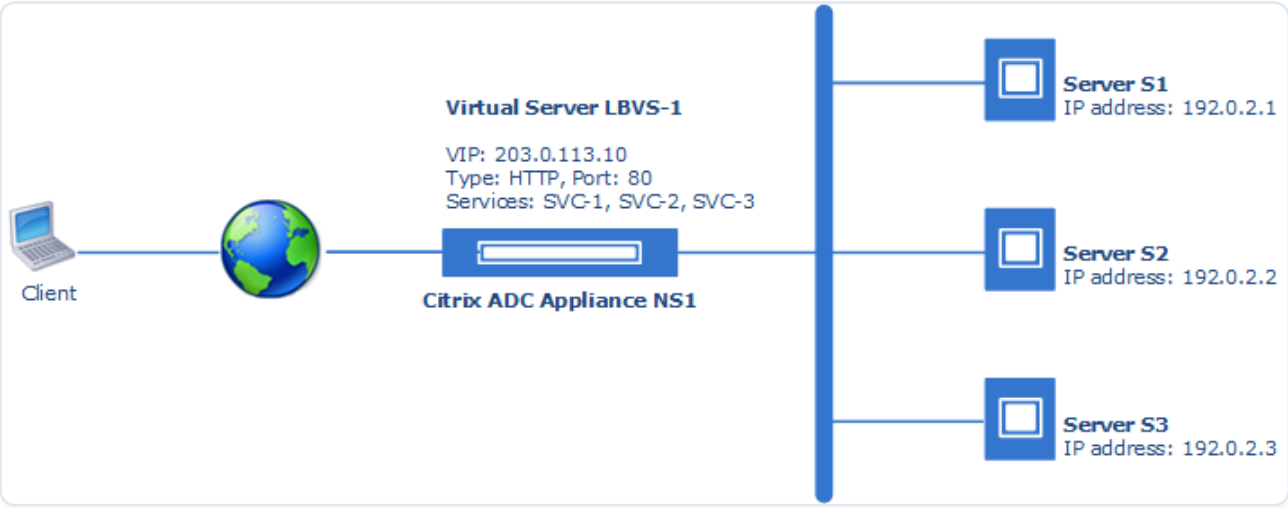
This section covers some use case scenarios to certain resources and scenarios. More scenarios will be added in future updates to this section.

Configure basic load balancing on a Citrix ADC VPX appliance

The load balancing feature of a Citrix ADC appliance distributes user requests for web pages and other protected applications across multiple servers that all host (or mirror) the same content. You use load balancing primarily to manage user requests to heavily used applications, preventing poor performance and outages and ensuring that users can access your protected applications. Load balancing also provides fault tolerance; when one server that hosts a protected application becomes unavailable, the feature distributes user requests to the other servers that host the same application.

A load balancing setup includes a load-balancing virtual server and multiple load-balanced application servers. The virtual server receives incoming client requests, uses the load balancing algorithm to select an application server, and forwards the requests to the selected application server.

Consider an example in which Example Corp hosts a site at `www.example.com`. To ensure application availability, the site is hosted on three servers, S1, S2, and S3. A load balancing virtual server, LBVS-1, on a Citrix ADC appliance NS-1 is used to load balance these servers. SVC-1, SVC-2, and SVC-3 are services created on Citrix ADC appliance NS-1 representing S1, S2, and S3.



Before you begin

Before you start configuring load balancing using NITRO REST APIs on a Citrix ADC VPX appliance, make sure that:

- You have deployed a Citrix ADC VPX appliance and the appliance is UP and running in your setup. For more information, see Deploy a Citrix ADC VPX instance.
- You have added a subnet IP (SNIP) address on the Citrix ADC appliance. A Citrix ADC uses a subnet IP (SNIP) address as a source IP address to proxy client connections to servers. For more information, see Configuring Subnet IP Addresses.
- You have a basic understanding of the load balancing feature of a Citrix ADC appliance. For more information, see:
  - Load Balancing
  - Load balance traffic on a Citrix ADC appliance
- You have a basic understading of the Citrix ADC NITRO REST APIs. For more information, see Citrix ADC NITRO API reference.

Configuration steps

Configuring load balancing on a Citrix ADC appliance using NITRO REST APIs consists of the following steps:

1. Create a load balancing virtual server
2. Create load balancing services
3. Bind the services to the load balancing server

Create a load balancing virtual server

A load balancing virtual server is an entity to which a client sends connection requests for a particular load-balanced website or application. A virtual server is represented by an IP address, a port, and a protocol.

To create a load balancing virtual server on a Citrix ADC VPX appliance, you use the Citrix ADC NITRO API `lbvserver` object.

For more information about the `lbvserver` object and its properties, see Citrix NITRO API reference for lbvserver.

Request structure

REQUEST FIELD	VALUE
HTTP Method	`POST`
URL	`http://<Citrix-ADC-IP-address(NSIP)>/nitro/v1/config/lbvserver`
Request Headers	`Content-Type: application/json`

Request Payload	`{ "lbvserver": { "name":"<value>", "servicetype":"<value>", "ipv46": "<value>", "port": "<value>", } }`
	`Example:`
	
	`{ "lbvserver": { "name":"LBVS-1", "servicetype":"HTTP", "ipv46": "203.0.113.10", "port": 443 } }`

Create load balancing services

A service is an entity, which represents a server or an application running on a server. A service identifies the servers IP address, a port, and a protocol.

To create a load balancing service on a Citrix ADC VPX appliance, you use the Citrix ADC NITRO API `service` object.

You must create a service for each server to be load balanced.

For more information about the `service` object and its properties, see Citrix NITRO API reference for service.

Request structure

REQUEST FIELD	VALUE
HTTP Method	`POST`
URL	`http://<Citrix-ADC-IP-address(NSIP)>/nitro/v1/config/service`
Request Headers	`Content-Type: application/json`

Request Payload	`{"service": { "name": "<service name>", "ip": "<IP address of the server>", "servicetype": "HTTP", "port": 443 }}`
	`Example:`
	
	`{"service": { "name": "SVC-1”, "ip": "192.0.2.10", "servicetype": "HTTP", "port": 443 }}`

Bind the services to the load balancing server

Bind the created services to the load balancing server.

To bind the created services to the load balancing server, you use the Citrix ADC NITRO API `lbvserver_service_binding` object.

For more information about the `lbvserver_service_binding` object and its properties, see Citrix NITRO API reference for lbvserver_service_binding.

Request structure

REQUEST FIELD	VALUE
HTTP Method	`PUT`

REQUEST FIELD	VALUE
URL	`http://<Citrix-ADC-IP-address(NSIP)>/nitro/v1/config/lbvserver_service_binding`
Request Headers	`Content-Type: application/json`

Request Payload	`{"lbvserver_service_binding": { "name": "<name of the virtual server>", "servicename": "Name of the service"}}`
	`Example:`
	
	`{"lbvserver_service_binding": { "name": "LBVS-1”"servicename": "SVC-1"}}`

Sample configuration

STEPS	CURL REQUESTS
Create a load balancing virtual server	`curl -v -X POST -H "Content-Type: application/json" -u nsroot:examplepassword http://192.0.0.33/nitro/v1/config/lbvserver -d '{ "lbvserver": { "name":"LBVS-EN", "servicetype":"HTTP", "ipv46": "203.0.113.10", "port": 80}'`
Create load balancing services	`curl -v -X POST -H "Content-Type:application/json" -u nsroot:examplepassword http://192.0.0.33/nitro/v1/config/service -d '{"service": { "name": "SVC-EN-1", "ip": "192.0.2.10", "servicetype": "HTTP", "port": 80 } }'` `curl -v -X POST -H "Content-Type:application/json" -u nsroot:examplepassword http://192.0.0.33/nitro/v1/config/service`

STEPS	CURL REQUESTS

	`-d '{"service": { "name": "SVC-EN-2", "ip": "192.0.2.30", "servicetype": "HTTP", "port": 80 } }'`
	
	`curl -v -X POST -H "Content-Type:application/json" -u nsroot:examplepassword http://192.0.0.33/nitro/v1/config/service -d '{"service": { "name": "SVC-EN-3", "ip": "192.0.2.30", "servicetype": "HTTP", "port": 80 } }'`

Bind the services to the load balancing server	`curl -v -X PUT -H "Content-Type:application/json" -u nsroot:examplepassword http://192.0.0.33/nitro/v1/config/lbvserver_service_binding -d '{"lbvserver_service_binding": { "name": "LBVS-EN", "servicename": "SVC-EN-1", "weight": "1" } }'`

Configure content switching in a Citrix ADC VPX Appliance

In today's complex Web sites, you may want to present different content to different users. For example:

- you may want to allow users from the IP range of a customer or partner to have access to a special Web portal.
- You may want to present content relevant to a specific geographical area to users from that area.
- You may want to present content in different languages to the speakers of those languages.
- You may want to present content tailored to specific devices, such as smartphones, to those who use the devices.

The Citrix ADC content switching feature enables the appliance to distribute client requests across multiple servers on the basis of specific content that you wish to present to those users.

A content switching configuration consists of a content switching virtual server, a load balancing setup consisting of load balancing virtual servers and services, and content switching policies. When a request reaches the content switching virtual server, the virtual server applies the associated content switching policies to that request. After it evaluates the policies, the content switching virtual server routes the request to the appropriate load balancing virtual server, which sends it to the appropriate service.

Consider an example in which Example Corp hosts a site at `www.example.com`. The site is hosted in two languages: English and French. The site in English content is hosted on two servers SVC-EN-1 and SVC-EN-2,and a load balancing virtual server, LBVS-EN, load balances these two servers. Similarly, the site in French content is hosted on two servers SVC-FR-1 and SVC-FR-2, and a load balancing virtual server, LBVS-FR, load balances these two servers. Both the load balancing servers LBVS-EN and LBVS-FR are associated with a content switching virtual server CSVS-1. Two content switching policies CSPOL-EN and CSPOL-FR are also associated with CSVS-1.

When an HTTP request reaches the CSVS-1, CSVS-1 uses the associated policies CSPOL-EN and CSPOL-FR to determine the language used in the request header. Based on the language determined, CSVS-1 routes the request to either LBVS-EN or LBVS-FR, which sends the request to one of its bound load balanced servers.

Before you begin

Before configuring content switching in a Citrix ADC VPX Appliance, make sure that:

- You have deployed a Citrix ADC VPX appliance and the appliance is UP and running in your setup. For more information, see Deploy a Citrix ADC VPX instance.
- You have a basic understanding of the load balancing feature of a Citrix ADC appliance. For more information, see:
  - Load Balancing
  - Load balance traffic on a Citrix ADC appliance
- You have a basic understanding of the content switching feature of a Citrix ADC appliance. For more information, see:
  - Content switching concept

- Configuring basic content switching

- You have a basic understading of the Citrix ADC NITRO REST APIs. For more information, see Citrix ADC NITRO API reference.

Configuration steps

Configuring content switching in a Citrix ADC appliance consists of the following steps:

1. Create a content switching virtual server
2. Create load balancing virtual servers
3. Create load balancing services
4. Bind the services to the load balancing servers
5. Create content switching policies
6. Bind content switching policies and load balancing virtual servers to the content switching virtual server

Create a content switching virtual server

To create a content switching virtual server, you use the `csvserver` NITRO API object. For more information about the csvserver object and its properties, see Citrix NITRO API reference for csvserver.

Curl request

```
curl -X POST -H "Content-Type: application/json" -u <username>:<password>
 http://<Citrix-ADC-IP-address(NSIP)>/nitro/v1/config/csvserver

-d '{"csvserver": { "name":"<value>", "servicetype":"<value>",
"ipv46":"<value>", "port":<value>}}'
```

Create load balancing virtual servers

To create a load balancing virtual server, you use the `lbvserver` NITRO API object.

For more information about the lbvserver object and its properties, see Citrix NITRO API reference for lbvserver.

Curl request

```
curl -v -X POST  -H "Content-Type: application/json" -u
<username>:<password> http://<Citrix-ADC-IP-address(NSIP)>/nitro/v1/
config/lbvserver -d '{ "lbvserver": { "name":"<value>",
 "servicetype":"<value>", "ipv46": "<value>", "port":<value>}'
```

Create load balancing services

To create a load balancing service, you use the `service` NITRO API object. You must create a service for each server to be load balanced.

For more information about the service object and its properties, see Citrix NITRO API reference for service.

Curl request

```
curl -v -X POST -H "Content-Type:application/json" -u
<username>:<password> http://<Citrix-ADC-IP-address(NSIP)>/nitro/v1/
config/service -d '{"service": { "name":"<value>", "ip":"<value>",
"servicetype":"<value>", "port":"<value>" } }'
```

Bind the services to the load balancing servers

To bind the created services to the load balancing servers, you use the `lbvserver_service_binding` NITRO API object.

For more information about the lbvserver_service_binding object and its properties, see Citrix NITRO API reference for lbvserver_service_binding.

Curl request

```
curl -v -X PUT -H "Content-Type:application/json" -u <username>:<password>
http://<Citrix-ADC-IP-address(NSIP)>/nitro/v1/config/
lbvserver_service_binding -d '{"lbvserver_service_binding":
{ "name":"<value>", "servicename":"<value>", "weight":"<value>" } }'
```

Create content switching policies

To create a content switching policy, you use the `cspolicy` NITRO API object.

For more information about the cspolicy object and its properties, see Citrix NITRO API reference for cspolicy.

Curl request

```
curl -v -X POST -H "Content-Type:application/json" -u
<username>:<password> http://<Citrix-ADC-IP-address(NSIP)>/nitro/v1/
config/cspolicy -d '{"cspolicy": { "policyname":"<value>",
"rule":"<value>" }' }'
```

Bind content switching policies and load balancing virtual servers to the content switching virtual server

To bind content switching policies and load balancing virtual servers to the content switching virtual server, you use the `csvserver_cspolicy_binding` NITRO API object.

For more information about the csvserver_cspolicy_binding object and its properties, see Citrix NITRO API reference for csvserver_cspolicy_binding.

Curl request

```
curl -v -X PUT -H "Content-Type:application/json" -u <username>:<password>
http://<Citrix-ADC-IP-address(NSIP)>/nitro/v1/config/
csvserver_cspolicy_binding -d '{"csvserver_cspolicy_binding": { "name":
"<value>", "policyname": "<value>", "targetlbvserver": "<value>",
"priority": "<value>" } }'
```

Sample configuration

STEPS	CURL REQUESTS
Create a content switching virtual server	`curl -X POST -H "Content-Type: application/json" -u nsroot:examplepassword http://192.0.0.33/nitro/v1/config/csvserver-d '{"csvserver": { "name": "CSVS-1", "servicetype": "HTTP", "ipv46": "203.0.113.5", "port": 80}}'`
Create load balancing virtual servers	`curl -v -X POST -H "Content-Type: application/json" -u`

STEPS	CURL REQUESTS
	`nsroot:examplepassword http://192.0.0.33//nitro/v1/config/lbvserver -d '{ "lbvserver": { "name":"LBVS-EN", "servicetype":"HTTP", "ipv46": "203.0.113.10", "port": 80}'` `curl -v -X POST -H "Content-Type: application/json" -u nsroot:examplepassword http://192.0.0.33//nitro/v1/config/lbvserver -d '{ "lbvserver": { "name":"LBVS-FR", "servicetype":"HTTP", "ipv46": "203.0.113.20", "port": 80}'`

Create load balancing services	`curl -v -X POST -H "Content-Type:application/json" -u nsroot:examplepassword http://192.0.0.33/nitro/v1/config/service -d '{"service": { "name": "SVC-EN-1", "ip": "192.0.2.10", "servicetype": "HTTP", "port": 80 } }'`
	`curl -v -X POST -H "Content-Type:application/json" -u nsroot:examplepassword http://192.0.0.33/nitro/v1/config/service -d '{"service": { "name": "SVC-EN-2", "ip": "192.0.2.20", "servicetype": "HTTP", "port": 80 } }`
	
	`curl -v -X POST -H "Content-Type:application/json" -u nsroot:examplepassword http://192.0.0.33/nitro/v1/config/service -d '{"service": { "name": "SVC-FR-1", "ip": "192.0.2.30",`

STEPS	CURL REQUESTS

	`"servicetype": "HTTP", "port": 80 } }'`
	
	`curl -v -X POST -H "Content-Type:application/json" -u nsroot:examplepassword http://192.0.0.33/nitro/v1/config/service -d '{"service": { "name": "SVC-FR-2", "ip": "192.0.2.40", "servicetype": "HTTP", "port": 80 } }`

Bind the services to the load balancing servers	`curl -v -X PUT -H "Content-Type:application/json" -u nsroot:examplepassword http://192.0.0.33/nitro/v1/config/lbvserver_service_binding -d '{"lbvserver_service_binding": { "name": "LBVS-EN", "servicename": "SVC-EN-1", "weight": "1" } }'`
	`curl -v -X PUT -H "Content-Type:application/json" -u nsroot:examplepassword http://192.0.0.33/nitro/v1/config/lbvserver_service_binding -d '{"lbvserver_service_binding": { "name": "LBVS-EN", "servicename": "SVC-EN-2", "weight": "1" } }'`
	
	`curl -v -X PUT -H "Content-Type:application/json" -u nsroot:examplepassword http://192.0.0.33/nitro/v1/config/lbvserver_service_binding -d '{"lbvserver_service_binding":`

STEPS	CURL REQUESTS

	`{ "name": "LBVS-FR", "servicename": "SVC-FR-1", "weight": "1" } }'`
	
	`curl -v -X PUT -H "Content-Type:application/json" -u nsroot:examplepassword http://192.0.0.33/nitro/v1/config/lbvserver_service_binding -d '{"lbvserver_service_binding": { "name": "LBVS-FR", "servicename": "SVC-FR-2", "weight": "1" } }'`

Create content switching policies	`curl -v -X POST -H "Content-Type:application/json" -u nsroot:examplepassword http://192.0.0.33/nitro/v1/config/cspolicy -d '{"cspolicy": { "policyname": "CSPOL-EN", "rule": "HTTP.REQ.URL.PATH_AND_QUERY.CONTAINS(\"en-us\")" } }'` `curl -v -X POST -H "Content-Type:application/json" -u nsroot:examplepassword http://192.0.0.33/nitro/v1/config/cspolicy -d '{"cspolicy": { "policyname": "CSPOL-FR", "rule": "HTTP.REQ.URL.PATH_AND_QUERY.CONTAINS(\"fr\")" } }'`
Bind content switching policies and load balancing virtual servers to the content switching virtual server	`curl -v -X PUT -H "Content-Type:application/json" -u nsroot:examplepassword http://192.0.0.33/nitro/v1/config/csvserver_cspolicy_binding -d '{"csvserver_cspolicy_binding": { "name": "CSVS-1", "policyname": "CSPOL-EN", "targetlbvserver": "LBVS-EN", "priority": "10" } }'`

STEPS	CURL REQUESTS
	`curl -v -X PUT -H "Content-Type:application/json" -u nsroot:examplepassword http://192.0.0.33/nitro/v1/config/csvserver_cspolicy_binding -d '{"csvserver_cspolicy_binding": { "name": "CSVS-1", "policyname": "CSPOL-FR", "targetlbvserver": "LBVS-FR", "priority": "20" } }'`

Log HTTP requests where the response is HTTP 5xx (server error)

In some scenarios in a Citrix ADC load balancing set up, a web server responds with a 5xx error code when it is unable to handle the request for reasons such as invalid requests, temporary overloading, or server maintenance. For example:

- 502 Bad Gateway. The server is acting as a gateway or proxy and received an invalid response from the upstream server.
- 503 Service Unavailable. The server is currently unavailable. The servers might be overloaded or down for maintenance.
- 504 Gateway Time-out. The server is acting as a gateway or proxy and did not receive a timely response from the upstream server.

You can log the HTTP requests for which the server responded with an HTTP 5xx error. You can then analyse these HTTP requests in a testing set up to troubleshoot the issues in server. To log the HTTP requests for which the server responded with an HTTP 5xx error, you must create an audit message action, create a rewrite policy and, associate the audit message action to the the rewrite policy. Then, you must bind the rewrite policy to the load balancing virtual server.

The Citrix ADC appliance uses the rewrite policy to identify the HTTP requests, for which the server responded with an HTTP 5xx error, in to the load balancing configuration. Then the appliance log these HTTP requests in a format defined in the audit message action.

Before you begin

Before configuring a Citrix ADC appliance to log HTTP requests, for which the server responded with an HTTP 5xx error, make sure that:

- You have deployed a Citrix ADC VPX appliance and the appliance is UP and running in your setup. For more information, see Deploy a Citrix ADC VPX instance.
- You have added a subnet IP (SNIP) address on the Citrix ADC appliance. A Citrix ADC uses a subnet IP (SNIP) address as a source IP address to proxy client connections to servers. For more information, see Configuring Subnet IP Addresses.
- You have added an HTTP load balancing configuration in the Citrix ADC appliance. For more information about load balancing configuration, see:
  - Load Balancing
  - Load balance traffic on a Citrix ADC appliance
- You have already configured audit logging (SYSLOG or NSLOG) in the Citrix ADC appliance.
  - Enabled `userdefinedauditlog` option in the related audit action server entity.
  - Bound the related audit policy to system global.

  For more information about Citrix ADC audit logging, see:
  - Audit logging concept
  - Configure Citrix ADC audit logging
- You have a basic understading of the Citrix ADC NITRO REST APIs. For more information, see Citrix ADC NITRO API reference.

Configuration steps

Configuring a Citrix ADC appliance to log HTTP requests, for which the server responded with an HTTP 5xx error, consists of the following steps:

1. Create an audit message action
2. Create a rewrite policy and specify the audit message action
3. Bind the rewrite policy to the load balancing virtual server

Create an audit message action

To create an audit message action, you use the `auditmessageaction` NITRO API object.

For more information about the auditmessageaction object and its properties, see Citrix NITRO API reference for auditmessageaction.

Curl request

```
curl -X POST -H "Content-Type: application/json" -u <username>:<password>
http://<Citrix-ADC-IP-address(NSIP)>/nitro/v1/config/auditmessageaction -d
'{ "auditmessageaction": { "name":"<value>", "loglevel":"<value>",
"stringbuilderexpr":"<value>" }}'
```

Create a rewrite policy and specify the audit message action

To create a rewrite policy and specify the audit message action, you use the `rewritepolicy` NITRO API object.

For more information about the rewritepolicy object and its properties, see Citrix NITRO API reference for rewritepolicy.

Curl request

```
curl -v -X POST  -H "Content-Type: application/json" -u
<username>:<password> http://<Citrix-ADC-IP-address(NSIP)>/nitro/v1/
config/rewritepolicy -d '{ "rewritepolicy": { "name":"<value>",
"rule":"<value>", "action":"<value>", "logaction":"<value>"}'
```

Bind the rewrite policy to the load balancing virtual server

To bind the rewrite policy to the load balancing virtual server, you use the `lbvserver_rewritepolicy_binding` NITRO API object.

For more information about the lbvserver_rewritepolicy_binding object and its properties, see Citrix NITRO API reference for lbvserver_rewritepolicy_binding.

Curl request

```
curl -v -X PUT -H "Content-Type:application/json" -u <username>:<password>
http://<Citrix-ADC-IP-address(NSIP)>/nitro/v1/config/
lbvserver_rewritepolicy_binding -d '{ "lbvserver_rewritepolicy_binding":
{ "name":"<value>", "policyname":"<value>", "priority":"<value>",
"gotopriorityexpression":"<value>", "bindpoint":"<value>" } }'
```

Sample configuration

STEPS	CURL REQUESTS
Create an audit message action	`curl -X POST -H "Content-Type: application/json" -u nsroot:examplepassword http://192.0.0.33/nitro/v1/config/auditmessageaction -d '{"auditmessageaction": { "name":"ADT-MSG-ACN-LOG-5XX", "loglevel":"WARNING", "stringbuilderexpr": ""\"Received \" + HTTP.RES.STATUS + \" response for URL : \" + HTTP.REQ.URL.HTTP_URL_SAFE""}}'`
Create a rewrite policy and specify the audit message action	`curl -v -X POST -H "Content-Type: application/json" -u nsroot:examplepassword http://192.0.0.33/nitro/v1/config/rewritepolicy -d '{ "rewritepolicy": { "name":"RWRT-POL-LOG-5XX", "rule":"HTTP.RES.IS_SERVER_ERROR", "action":"NOREWRITE", "logaction":"ADT-MSG-ACN-LOG-5XX"}'`
Bind the rewrite policy to the load balancing virtual server	`curl -v -X PUT -H "Content-Type:application/json" -u nsroot:examplepassword http://192.0.0.33/nitro/v1/config/lbvserver_rewritepolicy_binding -d '{ "lbvserver_rewritepolicy_binding": { "name":"LBVS-1", "policyname":"RWRT-POL-LOG-5XX", "priority": "100", "gotopriorityexpression": "END", "bindpoint": "RESPONSE" } }'`

Log transactions from a specific client in a load balancing configuration

You can log transactions from a specific client to analyse them to find any trends and metrics. This information can then be used to optimize the settings in the Citrix ADC and servers to improve efficiency in processing the client requests.

To log transactions from a specific client in a load balancing configuration, you must create an audit message action, create a rewrite policy and, associate the audit message action to the the rewrite policy. Then, you must bind the rewrite policy to the load balancing virtual server.

The Citrix ADC appliance uses the rewrite policy to identify transactions related to a specific client in a load balancing configuration. Then the appliance log these transactions in a format defined in the audit message action.

Before you begin

Before configuring a Citrix ADC appliance to log transactions from a specific client, make sure that:

- You have deployed a Citrix ADC VPX appliance and the appliance is UP and running in your setup. For more information, see Deploy a Citrix ADC VPX instance.
- You have a basic understanding of the load balancing feature of a Citrix ADC appliance. For more information, see:
  - Load Balancing
  - Load balance traffic on a Citrix ADC appliance
- You have already configured audit logging (SYSLOG or NSLOG) in the Citrix ADC appliance.
  - Enabled `userdefinedauditlog` option in the related audit action server entity.
  - Bound the related audit policy to system global.

  For more information about Citrix ADC audit logging, see:
  - Audit logging concept
  - Configure Citrix ADC audit logging
- You have a basic understading of the Citrix ADC NITRO REST APIs. For more information, see Citrix ADC NITRO API reference.

Configuration steps

Configuring a Citrix ADC appliance to log transactions from a specific client, consists of the following steps:

1. Create an audit message action
2. Create a rewrite policy and specify the audit message action
3. Bind the rewrite policy to the load balancing virtual server

Create an audit message action

To create an audit message action, you use the `auditmessageaction` NITRO API object.

For more information about the auditmessageaction object and its properties, see Citrix NITRO API reference for auditmessageaction.

Curl request

```
curl -X POST -H "Content-Type: application/json" -u <username>:<password>
http://<Citrix-ADC-IP-address(NSIP)>/nitro/v1/config/auditmessageaction -d
'{ "auditmessageaction": { "name":"<value>", "loglevel":"<value>",
"stringbuilderexpr":"<value>" }}'
```

Create a rewrite policy and specify the audit message action

To create a rewrite policy and specify the audit message action, you use the `rewritepolicy` NITRO API object.

For more information about the rewritepolicy object and its properties, see Citrix NITRO API reference for rewritepolicy.

Curl request

```
curl -v -X POST  -H "Content-Type: application/json" -u
<username>:<password> http://<Citrix-ADC-IP-address(NSIP)>/nitro/v1/
config/rewritepolicy -d '{ "rewritepolicy": { "name":"<value>",
"rule":"<value>", "action":"<value>", "logaction":"<value>"}'
```

Bind the rewrite policy to the load balancing virtual server

To bind the rewrite policy to the load balancing virtual server, you use the `lbvserver_rewritepolicy_binding` NITRO API object.

For more information about the lbvserver_rewritepolicy_binding object and its properties, see Citrix NITRO API reference for lbvserver_rewritepolicy_binding.

Curl request

```
curl -v -X PUT -H "Content-Type:application/json" -u <username>:<password>
http://<Citrix-ADC-IP-address(NSIP)>/nitro/v1/config/
lbvserver_rewritepolicy_binding -d '{ "lbvserver_rewritepolicy_binding":
{ "name":"<value>", "policyname":"<value>", "priority":"<value>",
"gotopriorityexpression":"<value>", "bindpoint":"<value>" } }'
```

Sample configuration

STEPS	CURL REQUESTS											
Create an audit message action	`curl -X POST -H "Content-Type: application/json" -u nsroot:exam	Client IP: "+ CLIENT.IP.SRC+"	Client TCP Source Port: "+ CLIENT.TCP.SRCPORT+"	Client TCP Destination Port: "+ CLIENT.TCP.DSTPORT+"	LBVSERVER NAME: "+ HTTP.REQ.LB_VSERVER.NAME+"	LBVSERVER IP: "+ CLIENT.IP.DST+"	Server IP: "+ SERVER.IP.DST+"	Server port: "+ SERVER.TCP.DSTPORT+"	HTTP Request Method: "+ HTTP.REQ.METHOD+"	HOST NAME: "+ HTTP.REQ.HOSTNAME+"	URL: "+ HTTP.REQ.URL+"	Response Code: "+ HTTP.RES.STATUS""}}'`

STEPS	CURL REQUESTS											
	ple pa ss wo rd htt p:// 19 2.0 .0. 33/ nitr o/ v1/ co nfi g/ au dit me ss ag ea cti on -d '{"a udi tm es sa ge act ion ": { "n											

STEPS	CURL REQUESTS	
	ame": "ADT-MSG-ACN-LOG-CLIENT", "loglevel":"WARNING", "stringbuilderexpr": """Date&Time	

STEPS	CURL REQUESTS											
	: "+ SYS. TIME +"											

STEPS	CURL REQUESTS	
Create a rewrite policy and specify the audit message action	`curl -v -X POST -H "Content-Type: application/json" -u nsroot:example pass`	

STEPS	CURL REQUESTS	
	`w or d ht tp :/ / 19 2. 0. 0. 33 / ni tr o/ v1 / co nf ig / re wr it ep ol ic y -d '{ " re wr it ep`	

STEPS	CURL REQUESTS	
	`o li cy ": { "n am e" :" RW RT - PO L- LO G- CL IE NT ", "r ul e" :" CL IE NT .I P. SR C. EQ (1 92 .0 .2`	

STEPS	CURL REQUESTS	
	`9.210)", "action":"NOREWRITE", "logaction":"ADT-MSG-ACN-LOG-CLIENT`	

STEPS	CURL REQUESTS	
	`"}'`	
Bind the rewrite policy to the load balancing virtual server	`curl -v -XPUT -H "Content-Type:application/json" -unsroot:example`	

STEPS	CURL REQUESTS	
	`p` `assword` `http://192.0.0.33/nitro/v1/config/lbvserver_rewritepolicy_`	

STEPS	CURL REQUESTS	
	`b` `in` `di` `ng` `-d` `'{` `"` `lb` `vs` `er` `ve` `r_` `re` `wr` `it` `ep` `ol` `ic` `y_` `bi` `nd` `in` `g"` `:` `{` `"n` `am` `e"` `:"` `LB` `VS` `-1` `",` `"p` `ol` `ic`	

STEPS	CURL REQUESTS	
	`y name": "RWRT-POL-LOG-CLIENT", "priority": "100", "gotopriorityexpression"`	

STEPS	CURL REQUESTS	
	`:"END","bindpoint":"RESPONSE" }}'`	

Disable a load balancing service in a Citrix ADC VPX Appliance

Network outages such as system upgrades or hardware maintenance of servers are scheduled at regular intervals. During this time, you must disable the Citrix ADC load balancing services representing these servers,

You can perform a hard shutdown or graceful shutdown of a service. Hard shutdown disables a service immediately disrupting any established sessions and any transactions in progress, which may result in data loss. Hard shutdown changes the state of the service to DOWN.

Graceful shutdown disables a service after a wait time or after all the current active client connections are closed by either the server or the client. Graceful shutdown first changes the state of the service to Transition Out of Service (TROFS) state till the wait time is over or all the active connections are closed, after which the state changes to DOWN.

Often, however, you cannot estimate the amount of time needed for all the connections to a service to complete the existing transactions. If a transaction is unfinished when the wait time expires, shutting down the service may result in data loss. In this case, you can specify the *graceful* option, so that the service is disabled only when all the current active client connections are closed by either the server or the client. See the following table for behavior if you specify a wait time in addition to graceful option.

Persistence is maintained according to the specified method even if you enable graceful shutdown. The system continues to serve all the persistent clients, including new connections from the clients, unless the service is marked DOWN during the graceful shutdown state as a result of the checks made by a monitor.

The following table describes the functionality of graceful shutdown of a service for different combinations of graceful and wait time values.

GRACEFUL	WAIT TIME	DESCRIPTION
Enabled	Specified	Service is shut down after the last of the current active client connections is served, even if the wait time has not expired. The appliance checks the status of the connections once every second. If the wait time expires, any open sessions are closed.
Disabled	Specified	Service is shut down only after the wait time expires, even if all established connections are served before expiration.
Enabled	Not specified	Service is shut down only after the last of the previously established connections is served, regardless of the time taken to serve the last connection.
Disabled	Not specified	No graceful shutdown. Service is shut down

GRACEFUL	WAIT TIME	DESCRIPTION
		immediately after the disable option is chosen or the disable command is issued. (The default wait time is zero seconds.)

Before you begin

Before you disable a load balancing service in a Citrix ADC VPX Appliance, make sure that:

- You have deployed a Citrix ADC VPX appliance and the appliance is UP and running in your setup. For more information, see Deploy a Citrix ADC VPX instance.
- You have a basic understanding of the load balancing feature of a Citrix ADC appliance. For more information, see:
- Load Balancing
- Load balance traffic on a Citrix ADC appliance
- You have an understanding of the following concepts related to a load balancing service:
  - various states of a load balancing service. For more information, Load balance service states.
  - Graceful shutdown of a load balancing service. For more information, Graceful shutdown of services.
- You have a basic understanding of the Citrix ADC NITRO REST APIs. For more information, see Citrix ADC NITRO API reference.

Steps to disable a load balancing service in a Citrix ADC VPX Appliance

To disable a load balance service in a Citrix ADC appliance, you use the *service* NITRO API object with action as *disable*. Optionally, for graceful shutdown of the service, set one or both of the following properties in the request payload:

NAME	DESCRIPTION
graceful	Shut down gracefully, not accepting any new connections, and disabling the service when all of its connections are closed.

NAME	DESCRIPTION
	Default value: NO Possible values: YES, NO
delay	Wait time, in seconds, allocated to the Citrix ADC for a graceful shutdown of the service. During this period, new requests are sent to the service only for clients who already have persistent sessions on the appliance. Requests from new clients are load balanced among other available services. After the delay time expires, no requests are sent to the service, and the service is marked as unavailable (OUT OF SERVICE). Default value: 0

For more information about the *service* object and its properties, see Citrix NITRO API reference for service.

Request components

REQUEST FIELD	VALUE
HTTP Method	`POST`
URL	`http://<Citrix-ADC-IP-address(NSIP)>/nitro/v1/config/service?action=disable`
Request Headers	`Content-Type: application/json`

Request Payload	`{"service": {"name":<value>,"delay":<value>,"graceful":<value>}}`
	Example:
	
	`{"service":{"name": "SVC-1”,"graceful": “Yes”}}`

Curl request

Use the following curl command syntax to disable a service in a Citrix ADC appliance:

```
curl -X POST -H "Content-Type: application/json" -u <username>:<password>
 http://<Citrix-ADC-IP-address(NSIP)>/nitro/v1/config/service?
action=disable -d '{"service": {"name": "<value>","graceful": "<value>",
"delay": "<value>"}}'
```

Examples

EXAMPLE DESCRIPTION	CURL REQUEST
Perform a graceful shutdown of a service named SVC-1 in a Citrix ADC appliance, which has the NSIP address of 192.0.0.33.	`curl -X POST -H "Content-Type: application/json" -u nsroot:examplepassword http://192.0.0.33/nitro/v1/config/service?action=disable -d '{"service": {"name": "SVC-1", "graceful": "Yes"}}'`
Perform a hard shutdown of a service named SVC-1 in a Citrix ADC appliance, which has the NSIP address of 192.0.0.33.	`curl -X POST -H "Content-Type: application/json" -u nsroot:examplepassword http://192.0.0.33/nitro/v1/config/service?action=disable -d '{"service": {"name": "SVC-1}}'`

Retrieve firmware and licensing information for a Citrix ADC VPX Appliance

Citrix supports NITRO REST APIs for retrieving firmware and licensing information for a Citrix ADC appliance. The firmware information includes the version and build number of the firmware running on the appliance. The licensing information includes the list of available ADC features, and the type and mode of the license used in the appliance.

Before you begin

Before you find firmware and licencing information for a Citrix ADC appliance, make sure that:

- You have deployed a Citrix ADC VPX appliance and the appliance is UP and running in your setup. For more information, see Deploy a Citrix ADC VPX instance.

- You have a basic understanding of Citrix ADC Licenses. For more information, see:
  - Citrix ADC Licensing
  - Manage Citrix ADC licenses using Citrix ADM

Retrieve firmware information for a Citrix ADC appliance

You use the _nsversion_NITRO API object to find information about the firmware running on a Citrix ADC appliance,.The Citrix ADC appliance responds with the version and build number of the firmware running on the appliance.

For more information about the _nsversion_object and its properties, see Citrix NITRO API reference for nsversion.

Request components

REQUEST FIELD	VALUE
HTTP Method	`GET`
URL	`http://<Citrix-ADC-IP-address(NSIP)>/nitro/v1/config/nsversion`
Request Headers	`Content-Type: application/json`

Curl request

```
curl -X GET -H "Content-Type: application/json" -u nsroot:examplepassword
 http://<Citrix-ADC-IP-address(NSIP)>/nitro/v1/config/nsversion
```

Retrieve licensing information for a Citrix ADC appliance

You use the *nslicense* NITRO API object to find information about the licenses on a Citrix ADC appliance.

The Citrix ADC appliance responds with the following information:

- List of ADC features available (marked as *true*) or not (marked as *false*) in the appliance
- `modelid`. This attribute represents different numbers for two types of licenses.
  - `Bandwidth licenses`. Specifies the throughput bandwidth licensed for this appliance. For example, for 20 Gbps, modelid: 20000

  - `vCPU licenses`. Specifies number of vCPUs licensed for this appliance. For example, for 4 vCPU, modelid: 4 vCPUs

- `licensingmode.` Thisattribute represents the mode of the license for this appliance:
  - Local
  - Pooled
  - CICO
  - EXPRESS
  - CPU
  - CPU-Local

For more information about the *nslicense* object and its properties, see Citrix NITRO API reference for nslicense.

Request components

REQUEST FIELD	VALUE
HTTP Method	`GET`

URL	`http://<Citrix-ADC-IP-address(NSIP)>/nitro/v1/config/nslicense`
	or
	
	`http://<Citrix-ADC-IP-address(NSIP)>/nitro/v1/config/nslicense?attrs=modelid,licensingmode`

Request Headers	`Content-Type: application/json`

Curl request

Use the following curl command syntax to find detailed licensing information for a Citrix ADC appliance:

```
curl -X GET -H "Content-Type: application/json" -u
<username>:<examplepassword>  http://<Citrix-ADC-IP-address(NSIP)>/nitro/
v1/config/nslicense
```

Use the following curl command syntax to find licensing information limited to modelid and licensing mode attributes:

```
curl -X GET -H "Content-Type: application/json" -u nsroot:examplepassword
 http://<Citrix-ADC-IP-address(NSIP)>/nitro/v1/config/nslicense?
attrs=modelid,licensingmode
```

Retrieve expiry information about SSL certificates in a Citrix ADC VPX Appliance

A typical deployment of a Citrix ADC appliance contains multiple load balancing configurations that process SSL transactions. SSL certificates bound to these configurations can expire at different times. You can retrieve the expiry information about SSL certificates in a Citrix ADC VPX Appliance. The expiry information helps you in renewing the SSL certificates on time.

Before you begin

Before youretrieve expiry information about SSL certificates in a Citrix ADC VPX Appliance, make sure that:

- You have deployed a Citrix ADC VPX appliance and the appliance is UP and running in your setup. For more information, see Deploy a Citrix ADC VPX instance.
- You have a basic understanding of SSL certificates in a Citrix ADC appliance. For more information, see: SSL certificates.

Steps to retrieve expiry information about SSL certificates in a Citrix ADC VPX Appliance

You use the *sslcertkey* NITRO API object to retrieve expiry information about the SSL certificates in a Citrix ADC appliance.

The Citrix ADC appliance responds with the following expiry information along with other details about SSL certificates in the appliance:

- `daystoexpiration`. This attribute represents thedays remaining for a SSL certificate to expire.

For more information about the *sslcertkey* object and its properties, see Citrix NITRO API reference for sslcertkey.

Request components

REQUEST FIELD	VALUE
HTTP Method	`GET`

URL	`http://<Citrix-ADC-IP-address(NSIP)>/nitro/v1/config/sslcertkey`
	or
	`http://<Citrix-ADC-IP-address(NSIP)>/nitro/v1/config/sslcertkey?attrs=certkey,cert,key,daystoexpiration`

Request Headers	`Content-Type: application/json`

Curl request

Use the following curl command syntax to retrieve detailed information about SSL certificates in a Citrix ADC appliance:

```
curl -X GET -H "Content-Type: application/json" -u
<username>:<examplepassword>  http://<Citrix-ADC-IP-address(NSIP)>/nitro/
v1/config/sslcertkey
```

Use the following curl command syntax to retrieve only the expiry information about SSL certificates in a Citrix ADC appliance:

```
curl -X GET -H "Content-Type: application/json" -u nsroot:examplepassword
 http://<Citrix-ADC-IP-address(NSIP)>/nitro/v1/config/sslcertkey?
attrs=certkey,cert,key,daystoexpiration
```

Example

EXAMPLE DESCRIPTION	CURL REQUEST	RESPONSE PAYLOAD
Retrieve only the expiry information about SSL certificates in a Citrix ADC	`curl -X GET -H "Content-Type: application/json" -u`	{ "errorcode": 0,

EXAMPLE DESCRIPTION	CURL REQUEST	RESPONSE PAYLOAD

appliance, which has Citrix ADC IP address (NSIP) of 192.0.0.33.	`nsroot:examplepassword` `http://192.0.0.33/nitro/v1/config/sslcertkey?attrs=certkey,cert,key,daystoexpiration`	"message": "Done",
		"severity": "NONE",
		"sslcertkey": [
		{
		"certkey": "ns-server-certificate",
		"cert": "ns-server.cert",
		"key": "ns-server.key",
		"daystoexpiration": 5509
		},
		{
		"certkey": "serverrsa_2048",
		"cert": "complete/server/server_rsa_2048.pem",
		"key": "complete/server/server_rsa_2048.ky",
		"daystoexpiration": 5652
		}
		]
		}

Performing a packet trace on a Citrix ADC VPX appliance

A Citrix ADC appliance provides a NITRO API object called `nstrace` to get a dump of the packets that are received and sent out by the appliance. The API stores the packets in trace files.

You can use these files to debug problems in the flow of packets in the Citrix ADC appliance. The trace files must be viewed with the Wireshark application.

Some salient aspects of the `nstrace` NITRO API object are:

- Can be configured to trace packets selectively by using classic expressions and default expressions.
- Can capture the trace in multiple formats: ns trace format (`.cap`) and TCP dump format (`.pcap`).

Before you begin

Before performing a packet trace on a Citrix ADC VPX appliance, note the following points:

- Make sure that you have deployed a Citrix ADC VPX appliance and the appliance is UP and running in your setup. For more information, see Deploy a Citrix ADC VPX instance.
- Make sure that you have a basic understanding of the `nstrace` feature of a Citrix ADC appliance. For more information, see:
  - How to record a packet trace on Citrix ADC.
- Make sure that you have a basic understanding of the Citrix ADC NITRO REST APIs. For more information, see Citrix ADC NITRO API reference.
- `nstrace` NITRO API is not available in the Java, C#, and Python SDKs.

Best practices

On a Citrix ADC appliance handling high volume of traffic per second, capturing traffic is a very resource intensive process. The impact to resources is mainly in terms of the CPU and the disk space. Disk space impact can be reduced by using filtering expressions. However, the impact on the CPU remains and sometimes causes a slight increase as the appliance now needs to process packets according to the filter before capturing them.

The best practices about packet tracing are:

- The duration for which the trace is run must be as limited as possible when you still ensure the packets of interest are captured.
- Schedule the tracing activity to happen at a time when the number of users (and hence the traffic) is greatly reduced, such as during off hours.

Steps for performing a packet trace

Performing a packet trace on a Citrix ADC VPX appliance consists of the following steps:

1. Start recording a packet trace
2. Retrieve the current state information of the packet trace recording
3. Stop recording a packet trace

Start recording a packet trace

To start recording a packet trace, you use the `nstrace` NITRO API object with action as `start`.

Packet traces are recorded in files in the `/var/nstrace/<date-timestamp>` directory of the appliance. The packet trace file name is of the form `nstrace<id>.cap`, where `id` is always 1 for a standalone appliance. In other words, packet trace file with the same name `nstrace1.cap` is always generated for a standalone appliance.

For more information about the `nstrace` object and its properties, see Citrix NITRO API reference for nstrace.

Request components

REQUEST FIELD	VALUE
HTTP Method	`POST`
URL	`http://<Citrix-ADC-IP-address(NSIP)>/nitro/v1/config/nstrace?action=start`
Request Headers	`Content-Type: application/json`

Request Payload	`{"nstrace":{"size":<value>, "mode":<value>, ... }}`
	Example:
	
	`{"nstrace":{"size":0}}`

Curl request

```
curl -X POST -H "Content-Type: application/json" -u nsroot:examplepassword
http://<Citrix-ADC-IP-address(NSIP)>/nitro/v1/config/nstrace?action=start
 -d '{"nstrace":{"size":<value>, "mode":<value>, ... }}'
```

Example

```
curl -X POST -H "Content-Type: application/json" -u nsroot:examplepassword
http://192.0.0.33/nitro/v1/config/nstrace?action=start  -d '{"nstrace":
{"size":0}}'
```

Retrieve the current state information of the packet trace recording

To retrieve the current state information of the packet trace recording, you use the `nstrace` NITRO API object along with HTTP method as `GET`.

The Citrix ADC appliance responds with the following information:

- `state`. This attribute shows the current state information of the packet trace recording. Possible values: RUNNING, STOPPED
- Other attributes settings that are used in the current packet trace recording in running state. If the packet trace recording is not running(state shown as STOPPED), default settings are shown for the attributes.

For more information about the `nstrace` object and its properties, see Citrix NITRO API reference for nstrace.

Request components

REQUEST FIELD	VALUE
HTTP Method	`GET`
URL	`http://<Citrix-ADC-IP-address(NSIP)>/nitro/v1/config/nstrace`
Request Headers	`Content-Type: application/json`

Curl request

```
curl -X GET -H "Content-Type: application/json" -u nsroot:examplepassword
http://<Citrix-ADC-IP-address(NSIP)>/nitro/v1/config/nstrace
```

Examples

EXAMPLE DESCRIPTION	CURL REQUEST	RESPONSE PAYLOAD

Retrieve the current state information and other attribute settings of the packet trace recording in a Citrix ADC appliance, which has Citrix ADC IP address (NSIP) of 192.0.0.33.	`curl -X GET -H "Content-Type: application/json" -u nsroot:examplepassword http://192.0.0.33/nitro/v1/config/nstrace`	{
		"errorcode": 0,
		"message": "Done",
		"severity": "NONE",
		"nstrace": {
		"state": "RUNNING",
		"scope": "LOCAL",
		"tracelocation": "/var/nstrace/18Feb2021_20_08_25/...",
		"nf": "24",
		"time": "3600",
		"size": "0",
		"mode": [
		"TXB",
		"NEW_RX"
		],
		"traceformat": "NSCAP",
		"pernic": "DISABLED",
		"filename": "18Feb2021_20_08_25",
		"link": "DISABLED",
		"merge": "ONSTOP",

EXAMPLE DESCRIPTION	CURL REQUEST	RESPONSE PAYLOAD
		"doruntimecleanup": "ENABLED", "tracebuffers": "5000", "skiprpc": "DISABLED", "skiplocalssh": "DISABLED", "capsslkeys": "DISABLED", "capdroppkt": "DISABLED", "inmemorytrace": "DISABLED" } }

Retrieve only the current state information of the packet trace recording in a Citrix ADC appliance, which has Citrix ADC IP address (NSIP) of 192.0.0.33.	`curl -X GET -H "Content-Type: application/json" -u nsroot:examplepassword http://192.0.0.33/nitro/v1/config/nstrace`	{
		"errorcode": 0,
		"message": "Done",
		"severity": "NONE",
		"nstrace": {
		"state": "RUNNING"
		}
		}

Stop recording a packet trace

To stop recording a packet trace, you use the `nstrace` NITRO API object with action as `stop`.

For more information about the `nstrace` object and its properties, see Citrix NITRO API reference for nstrace.

Request components

REQUEST FIELD	VALUE
HTTP Method	`POST`
URL	`http://<Citrix-ADC-IP-address(NSIP)>/nitro/v1/config/nstrace?action=stop`
Request Headers	`Content-Type: application/json`
Request Payload	`{"nstrace":{}}`

Curl request

```
curl -X POST -H "Content-Type: application/json" -u nsroot:examplepassword
http://<Citrix-ADC-IP-address(NSIP)>/nitro/v1/config/nstrace?action=stop
 -d '{"nstrace":{}}'
```

Example

```
curl -X POST -H "Content-Type: application/json" -u nsroot:examplepassword
   -d '{"nstrace":{}}'
```

miscellaneous use cases

This section covers some miscellaneous use cases.

Managing a Citrix ADC Cluster

For managing clusters, you can add or remove a cluster instance or an individual node and perform a few other instance or node operations such as viewing instance or node properties. You can also configure the cluster IP address. Other cluster-management tasks include joining a Citrix ADC appliance to the cluster and configuring a linkset. For detailed information and best practices, see Clustering.

Cluster Instance Operations

This topic covers cluster instance operations by using REST APIs through HTTP or SDKs.

- `Using REST APIs through HTTP`

All operations on a cluster instance must be performed on the clusterinstance object.

For example, to create a cluster instance with ID 1, connect to the Citrix ADC appliance that you are first adding to the cluster.

- `Request`

  `HTTP Method:` POST

`URL:` http://<Citrix-ADC-IP-address(NSIP)>/nitro/v1/config/clusterinstance

`Request Headers:`

Cookie:NITRO_AUTH_TOKEN=<tokenvalue>

Content-Type:application/json

`Request Payload:`

```
{

    "clusterinstance":

    {

    "clid":1,

    "preemption":"ENABLED"

    }

}
```

- `Response`

  `HTTP Status Code on Success:` 201 Created

`HTTP Status Code on Failure:` 4xx <string> (for general HTTP errors) or 5xx <string> (for Citrix-ADC-specific errors). The response payload provides details of the error.

- `Using REST APIs through SDKs`

  The com.citrix.netscaler.nitro.resource.config.cluster.clusterinstance class provides APIs to manage a cluster instance.

The following sample code creates a cluster instance with ID 1.

`Java - Sample code to create a cluster instance`

```
clusterinstance new_cl_inst_obj = new clusterinstance();



//Set the properties of the cluster instance locally



new_cl_inst_obj.set_clid(1);

new_cl_inst_obj.set_preemption("ENABLED");



//Upload the cluster instance



clusterinstance.add(ns_session,new_cl_inst_obj);
```

`.NET - Sample code to create a cluster instance`

```
clusterinstance new_cl_inst_obj = new clusterinstance();



//Set the properties of the cluster instance locally



new_cl_inst_obj.clid = 1;



new_cl_inst_obj.preemption = "ENABLED";
```

```
//Upload the cluster instance



clusterinstance.add(ns_session,new_cl_inst_obj);
```

`Python - Sample code to create a cluster instance`

```
new_cl_inst_obj = clusterinstance()



# Set the properties of the cluster instance locally



new_cl_inst_obj.clid = 1



# Upload the cluster instance



clusterinstance.add(ns_session, new_cl_inst_obj)
```

Cluster Node Operations

This topic covers cluster node operations by using REST APIs through HTTP or SDKs.

- `Using REST APIs through HTTP`

  All operations on a cluster node must be performed on the clusternode object. For example, to add a Citrix ADC appliance with NSIP address 10.102.29.60 to the cluster.

- `Request`

  `HTTP Method:` POST

`URL:` http://<Citrix-ADC-IP-address(NSIP)>/nitro/v1/config/clusternode

`Request Headers:`

Cookie:NITRO_AUTH_TOKEN=<tokenvalue>

Content-Type:application/json

`Request Payload:`

```
{

"clusternode":

    {

    "nodeid":1,

    "ipaddress":"10.102.29.60",

    "state":"ACTIVE",

    "backplane":"1/1/2"

    }

}
```

- `Response`

  `HTTP Status Code on Success:` 201 Created

`HTTP Status Code on Failure:` 4xx <string> (for general HTTP errors) or 5xx <string> (for Citrix-ADC-specific errors). The response payload provides details of the error.

- `Using REST APIs through SDKs`

The com.citrix.netscaler.nitro.resource.config.cluster.clusternode class provides APIs to manage cluster nodes.

The following sample code adds a cluster node with NSIP address 10.102.29.60.

`Java - Sample code to add a cluster node`

```
clusternode new_cl_node_obj = new clusternode();
```

```
//Set the properties of the cluster node locally

new_cl_node_obj.set_nodeid(0);

new_cl_node_obj.set_ipaddress("10.102.29.60");

new_cl_node_obj.set_state("ACTIVE");

new_cl_node_obj.set_backplane("0/1/1");

//Upload the cluster node

clusternode.add(ns_session,new_cl_node_obj);
```

`.NET - Sample code to add a cluster node`

```
clusternode new_cl_node_obj = new clusternode();

//Set the properties of the cluster node locally

new_cl_node_obj.nodeid = 0;

new_cl_node_obj.ipaddress = "10.102.29.60";
```

```
new_cl_node_obj.state = "ACTIVE";

new_cl_node_obj.backplane = "0/1/1";

//Upload the cluster node

clusternode.add(ns_session,new_cl_node_obj);
```

`Python - Sample code to add a cluster node`

```
new_cl_node_obj = clusternode()

# Set the properties of the cluster node locally

new_cl_node_obj.nodeid = 0

new_cl_node_obj.ipaddress = "10.102.29.60"

new_cl_node_obj.state = "ACTIVE"

new_cl_node_obj.backplane = "0/1/1"

# Upload the cluster node
```

```
clusternode.add(ns_session, new_cl_node_obj)
```

Add a Cluster IP Address

This topic covers adding a cluster IP address by using REST APIs through HTTP or SDKs.

- `Using REST APIs through HTTP`

  To define a cluster IP address, specify the required parameters in the nsip object. For example, to configure a cluster IP address.

- `Request`

  `HTTP Method:` POST

`URL:` http://<Citrix-ADC-IP-address(NSIP)>/nitro/v1/config/nsip

`Request Headers:`

Cookie:NITRO_AUTH_TOKEN=<tokenvalue>

Content-Type:application/json

`Request Payload:`

```
{

"nsip":

    {

    "ipaddress":"10.102.29.61",

    "netmask":"255.255.255.255",

    "type":"CLIP"

    }

}
```

- `Response`

  `HTTP Status Code on Success:` 201 Created

`HTTP Status Code on Failure:` 4xx <string> (for general HTTP errors) or 5xx <string> (for Citrix-ADC-specific errors). The response payload provides details of the error.

- `Using REST APIs through SDKs`

  The com.citrix.netscaler.nitro.resource.config.ns.nsip class provides the add() API to configure an IP address. To configure the IP address as a cluster IP address, you must specify the type as CLIP.

The following sample code configures a cluster IP address on Citrix ADC appliance with IP address 10.102.29.60.

`Java - Sample code to add a cluster IP address`

```
nsip new_nsip_obj = new nsip();



//Set the properties locally



new_nsip_obj.set_ipaddress("10.102.29.61");



new_nsip_obj.set_netmask("255.255.255.255");



new_nsip_obj.set_type("CLIP");



//Upload the cluster node
```

```
nsip.add(ns_session,new_nsip_obj);
```

`.NET - Sample code to add a cluster IP address`

```
nsip new_nsip_obj = new nsip();


//Set the properties locally


new_nsip_obj.ipaddress = "10.102.29.61";


new_nsip_obj.netmask = "255.255.255.255";


new_nsip_obj.type = "CLIP";


//Upload the cluster node


nsip.add(ns_session,new_nsip_obj);
```

`Python - Sample code to add a cluster IP address`

```
new_nsip_obj = nsip()


# Set the properties locally


new_nsip_obj.ipaddress = "10.102.29.61"
```

```
new_nsip_obj.netmask = "255.255.255.255"

new_nsip_obj.type = "CLIP"

# Upload the cluster node

nsip.add(ns_session, new_nsip_obj)
```

Add a Spotted IP Address

This topic covers adding a spotted IP address by using REST APIs through HTTP or SDKs.

- `Using REST APIs through HTTP`

  To configure an IP address as spotted, specify the required parameters in the nsip object. This configuration must be done on the cluster IP address.

For example, to configure a spotted SNIP address on a node with ID 1.

- `Request`

  `HTTP Method:` POST

`URL:` http://<cluster-ip-address\>/nitro/v1/config/nsip

`Request Headers:`

Cookie:NITRO_AUTH_TOKEN=<tokenvalue>

Content-Type:application/json

`Request Payload:`

```
{

"nsip":

    {

    "ipaddress":"10.102.29.77",

    "netmask":"255.255.255.0",

    "type":"SNIP",

    "ownernode":1

    }

}
```

- `Response`

  `HTTP Status Code on Success:` 201 Created

`HTTP Status Code on Failure:` 4xx <string> (for general HTTP errors) or 5xx <string> (for Citrix-ADC-specific errors). The response payload provides details of the error.

- `Using REST APIs through SDKs`

  The com.citrix.netscaler.nitro.resource.config.ns.nsip class provides the add() API to configure an IP address. To configure the IP address as spotted, you must specify the ID of the node that must own the IP address. This configuration must be done on the cluster IP address.

The following sample code configures a spotted SNIP address on a node with ID 1.

`Java - Sample code to configure a spotted IP address`

```
nsip new_nsip_obj = new nsip();



//Set the properties locally
```

```
new_nsip_obj.set_ipaddress("10.102.29.77");


new_nsip_obj.set_netmask("255.255.255.0");


new_nsip_obj.set_type("SNIP");


new_nsip_obj.set_ownernode(1);


//Upload the cluster node


nsip.add(ns_session,new_nsip_obj);
```

`.NET - Sample code to configure a spotted IP address`

```
nsip new_nsip_obj = new nsip();


//Set the properties locally


new_nsip_obj.ipaddress = "10.102.29.77";


new_nsip_obj.netmask = "255.255.255.0";


new_nsip_obj.type = "SNIP";
```

```
new_nsip_obj.ownernode = 1;

//Upload the cluster node

nsip.add(ns_session,new_nsip_obj);
```

`Python - Sample code to configure a spotted IP address`

```
# Add a spotted IP address

new_nsip_obj = nsip()

# Set the properties locally

new_nsip_obj.ipaddress = "10.102.29.77"

new_nsip_obj.netmask = "255.255.255.0"

new_nsip_obj.type = "SNIP"

new_nsip_obj.ownernode = 1
```

```
# Upload the cluster node



nsip.add(ns_session, new_nsip_obj)
```

Join Citrix ADC Appliance to Cluster

This topic covers adding a Citrix ADC appliance to a cluster by using REST APIs through HTTP or SDKs.

- `Using REST APIs through HTTP`

  To join an appliance to a cluster, specify the required parameters in the cluster object. For example, to join a Citrix ADC appliance to a cluster.

- `Request`

  `HTTP Method:` POST

`URL:` http://<Citrix-ADC-IP-address(NSIP)>/nitro/v1/config/cluster

`Request Headers:`

Cookie:NITRO_AUTH_TOKEN=<tokenvalue>

Content-Type:application/json

`Request Payload:`

```
{

"cluster":

    {

    "clip":"10.102.29.61",

    "password":"verysecret"

    }
```

```
}
```

- `Response`

  `HTTP Status Code on Success:` 201 Created

`HTTP Status Code on Failure:` 4xx <string> (for general HTTP errors) or 5xx <string> (for Citrix-ADC-specific errors). The response payload provides details of the error.

- `Using REST APIs through SDKs`

  The com.citrix.netscaler.nitro.resource.config.cluster.cluster class provides the join() API to join a Citrix ADC appliance to the cluster. You must specify the cluster IP address and the nsroot password of the configuration coordinator.

The following sample code joins a Citrix ADC appliance to a cluster.

`Java - Sample code to join an appliance to a cluster`

```
cluster new_cl_obj = new cluster();



//Set the properties of the cluster  locally



new_cl_obj.set_clip("10.102.29.61");



new_cl_obj.set_password("verysecret");



//Upload the cluster



cluster.add(ns_session,new_cl_obj);
```

`.NET - Sample code to join an appliance to a cluster`

```
cluster new_cl_obj = new cluster();



//Set the properties of the cluster locally



new_cl_obj.clip = "10.102.29.61";



new_cl_obj.password = "verysecret";



//Upload the cluster node



cluster.add(ns_session,new_cl_node_obj);
```

`Python - Sample code to join an appliance to a cluster`

```
new_cl_obj = cluster()



# Set the properties of the cluster locally



new_cl_obj.clip = "10.102.29.61"



new_cl_obj.password = "verysecret"



# Upload the cluster
```

```
cluster.add(ns_session, new_cl_obj)
```

Linkset Operations

This topic covers some linkset operations by using REST APIs through HTTP or SDKs.

- `Using REST APIs through HTTP`

  To configure a linkset, do the following:

Create a linkset by specifying the required parameters in the linkset object. For example, to add a linkset LS/1:

`Request:`

`HTTP Method:` POST

`URL:` http://<cluster-ip-address\>/nitro/v1/config/linkset

`Request Headers:`

Cookie:NITRO_AUTH_TOKEN=<tokenvalue>

Content-Type:application/json

- `Request Payload`

  ```
  ```

{ "linkset": { "id":"LS/1" } }

```
-   `Response`


    `HTTP Status Code on Success:` 201 Created


`HTTP Status Code on Failure:` 4xx &lt;string&gt; (for general HTTP
errors) or 5xx &lt;string&gt; (for Citrix-ADC-specific errors). The
```

```
response payload provides details of the error.



Bind the required interfaces to the linkset by specifying the interfaces
in the linkset_interface_binding object.For example, to bind interfaces
1/1/2 and 2/1/2 to linkset LS/1.



-  `Request`



    `HTTP Method:` PUT



`URL:` http://\&lt;cluster-ip-address\>/nitro/v1/config/
linkset_interface_binding/LS%2F1?action=bind

`Note.` The linkset name (LS/1), must be URL encoded as LS%2F1.



`Request Headers:`



Cookie:NITRO_AUTH_TOKEN=\&lt;tokenvalue>



Content-Type:application/json



`Request Payload:`



```json

{
```
```

```
"linkset_interface_binding":

    {

    "id":"LS/1",

    "ifnum":"1/1/2 2/1/2"

    }

}
```

- `Response`

  `HTTP Status Code on Success:` 200 Ok

`HTTP Status Code on Failure:` 4xx <string> (for general HTTP errors) or 5xx <string> (for Citrix-ADC-specific errors). The response payload provides details of the error.

- `Using REST APIs through SDKs`

  The com.citrix.netscaler.nitro.resource.config.network.linkset class provides the APIs to manage linksets.

To configure a linkset, do the following:

1. Add a linkset by invoking the add() method of the linkset class.
2. Bind the interfaces to the linkset using the add() method of the linkset_interface_binding class.

The following sample code creates a linkset LS/1 and bind interfaces 1/1/2 and 2/1/2 to it.

`Java - Sample code to configure linksets`

```
linkset new_linkset_obj = new linkset();



new_linkset_obj.set_id("LS/1");



linkset.add(ns_session,new_linkset_obj);
```

```
//Bind the interfaces to the linkset

linkset_interface_binding new_linkif_obj = new
linkset_interface_binding();

new_linkif_obj.set_id("LS/1");

new_linkif_obj.set_ifnum("1/1/2 2/1/2");

linkset_interface_binding.add(ns_session,new_linkif_obj);
```

`.NET - Sample code to configure linksets`

```
linkset new_linkset_obj = new linkset();

new_linkset_obj.id = "LS/1";

linkset.add(ns_session,new_linkset_obj);

//Bind the interfaces to the linkset

linkset_interface_binding new_linkif_obj = new
linkset_interface_binding();
```

```
new_linkif_obj.id = "LS/1";

new_linkif_obj.ifnum = "1/1/2 2/1/2";

linkset_interface_binding.add(ns_session,new_linkif_obj);
```

`Python - Sample code to configure linksets`

```
# Create a new linkset

new_linkset_obj = linkset()

new_linkset_obj.id = "LS/1"

linkset.add(ns_session, new_linkset_obj)

# Bind the interfaces to the linkset

new_linkif_obj = linkset_interface_binding()

new_linkif_obj.id = "LS/1"
```

```
new_linkif_obj.ifnum = "1/1/2 2/1/2"



linkset_interface_binding.add(ns_session, new_linkif_obj)
```

Configuring Admin Partitions

To create an admin partition, you must perform a set of operations on the default partition. To understand this procedure, let us consider a company that has two departments each of which has an application that requires the Citrix ADC functionality. The Citrix ADC admin wants to have a different partition for each department so that there is isolation of users and configurations. For detailed information and best practices, see Admin Partitions.

Creating an Admin Partition

While creating an admin partition, you must also specify the system resources that must be allocated to that partition.

- `Using REST APIs through HTTP`

  The following example creates an admin partition named partition-dept1.

- `Request`

  `HTTP Method:` POST

`URL:` http://<Citrix-ADC-IP-address(NSIP)>/nitro/v1/config/nspartition

`Request Headers:`

Cookie:NITRO_AUTH_TOKEN=<tokenvalue>

Content-Type:application/json

`Request Payload:`

```
{

"nspartition":

{
```

```
    "partitionname":"partition-dept1",

    "maxbandwidth":"10240",

    "minbandwidth":"10240",

    "maxconn":"1024",

    "maxmemlimit":"10"

}

}
```

- `Response`

  `HTTP Status Code on Success:` 201 Created

`HTTP Status Code on Failure:` 4xx <string> (for general HTTP errors) or 5xx <string> (for Citrix-ADC-specific errors). The response payload provides details of the error.

- `Using REST APIs through SDKs`

  The following sample code creates an admin partition named partition-dept1.

`Java - Sample code to create an admin partition`

```
nspartition nspartitionObject = new nspartition();



nspartitionObject.set_partitionname("partition-dept1");



nspartitionObject.set_maxbandwidth(10240);



nspartitionObject.set_maxconn(1024);
```

```
nspartitionObject.set_maxmemlimit(10);


nspartitionObject.set_minbandwidth(1240);


base_response result = nspartition.add(nitroService, nspartitionObject);
```

`.NET - Sample code to create an admin partition`

```
nspartition nspartitionObject = new nspartition();


nspartitionObject.partitionname = "partition-dept1";


nspartitionObject.maxbandwidth = 10240;


nspartitionObject.maxconn = 1024;


nspartitionObject.maxmemlimit = 10;


nspartitionObject.minbandwidth = 1240;


base_response result = nspartition.add(nitroService, nspartitionObject);
```

`Python - Sample code to create an admin partition`

```
nspartitionObject = nspartition()


nspartitionObject.partitionname = "partition-dept1"


nspartitionObject.maxbandwidth = 10240


nspartitionObject.maxconn = 1024


nspartitionObject.maxmemlimit = 10


nspartitionObject.minbandwidth = 1240


result = nspartition.add(nitroService, nspartitionObject)
```

Associating Users with Partitions

Associate the appropriate users with the partition.

- `Using REST APIs through HTTP`

  The following example associates user1 to a partition named partition-dept1.

- `Request`

  `HTTP Method:` PUT

`URL:` http://<Citrix-ADC-ip-address(NSIP)\>/nitro/v1/config/systemuser_nspartition_binding/user1

`Request Headers:`

Cookie:NITRO_AUTH_TOKEN=<tokenvalue>

Content-Type:application/json

`Request Payload:`

```
{

    "systemuser_nspartition_binding":

    {

    "username":"user1",

    "partitionname":"partition-dept1"

    }

}
```

- `Response`

  `HTTP Status Code on Success:` 201 Created

`HTTP Status Code on Failure:` 4xx <string> (for general HTTP errors) or 5xx <string> (for Citrix-ADC-specific errors). The response payload provides details of the error.

- `Using REST APIs through SDKs`

  The following sample code associates "user1" to a partition named "partition-dept1".

`Java - Sample code for associating user with partition`

```
systemuser_nspartition_binding systemuser_nspartition_binding_object = new
systemuser_nspartition_binding();



systemuser_nspartition_binding_object.set_partitionname("partition-
dept1");



systemuser_nspartition_binding_object.set_username("user1");
```

```
base_response result = systemuser_nspartition_binding.add(nitroService,
systemuser_nspartition_binding_object);
```

`.NET - Sample code for associating user with partition`

```
systemuser_nspartition_binding systemuser_nspartition_binding_object = new
systemuser_nspartition_binding();



systemuser_nspartition_binding_object.partitionname = "partition-dept1";



systemuser_nspartition_binding_object.username = "user1";



base_response result = systemuser_nspartition_binding.add(nitroService,
systemuser_nspartition_binding_object);
```

`Python - Sample code for associating user with partition`

```
systemuser_nspartition_binding_object =  systemuser_nspartition_binding()



systemuser_nspartition_binding_object.partitionname = "partition-dept1"



systemuser_nspartition_binding_object.username = "user1"



result = systemuser_nspartition_binding.add(nitroService,
systemuser_nspartition_binding_object)
```

Specifying Command Policy for Partition Users

Associate an appropriate command policy to the admin partition user.

- `Using REST APIs through HTTP`

  The following example associates the command policy partition-admin to user1.

- `Request`

  `HTTP Method:` PUT

`URL:` http://<Citrix-ADC-IP-address(NSIP)>/nitro/v1/config/systemuser_systemcmdpolicy_binding/user1

`Request Headers:`

Cookie:NITRO_AUTH_TOKEN=<tokenvalue>

Content-Type:application/json

`Request Payload:`

```
{

    "systemuser_systemcmdpolicy_binding":

    {

    "username":"user1",

    "policyname":"partition-admin",

    "priority":"1"

    }

}
```

- `Response`

  `HTTP Status Code on Success:` 201 Created

`HTTP Status Code on Failure:` 4xx <string> (for general HTTP errors) or 5xx <string> (for Citrix-ADC-specific errors). The response payload provides details of the error.

- `Using REST APIs through SDKs`

  The following sample code associates the command policy "partition-admin" to "user1".

`Java - Sample code to specify command policy for partition user`

```
systemuser_systemcmdpolicy_binding binding_object = new
systemuser_systemcmdpolicy_binding();



binding_object.set_username("user1");



binding_object.set_policyname("partition-admin");



binding_object.set_priority(1);



base_response result =
systemuser_systemcmdpolicy_binding.add(nitroService,binding_object);
```

`.NET - Sample code to specify command policy for partition user`

```
systemuser_systemcmdpolicy_binding binding_object = new
systemuser_systemcmdpolicy_binding();



binding_object.username = "user1";



binding_object.policyname = "partition-admin";



binding_object.priority = 1;
```

```
base_response result =
systemuser_systemcmdpolicy_binding.add(nitroService,binding_object);
```

`Python - Sample code to specify command policy for partition user`

```
binding_object = systemuser_systemcmdpolicy_binding()



binding_object.username = "user1"



binding_object.policyname = "partition-admin"



binding_object.priority = 1



result =
systemuser_systemcmdpolicy_binding.add(nitroService,binding_object)
```

Specifying the Admin Partition VLAN or Bridgegroup

Specify the VLANs or bridgegroups to be associated with the partition. This step ensures network isolation of the traffic. Traffic received on the interfaces of the VLAN or bridgegroup is isolated from the traffic of other partitions.

- `Using REST APIs through HTTP`

  The following example specifies a VLAN for an admin partition.

- `Request`

  `HTTP Method:` PUT

`URL:` http://<Citrix-ADC-IP-address(NSIP)>/nitro/v1/config/nspartition_vlan_binding/partition-dept1

`Request Headers:`

Cookie:NITRO_AUTH_TOKEN=<tokenvalue>

Content-Type:application/json

`Request Payload:`

```
{

    "nspartition_vlan_binding":

    {

    "partitionname":"partition-dept1",

    "vlan":"2"

    }

}
```

- `Response`

  `HTTP Status Code on Success:` 201 Created

`HTTP Status Code on Failure:` 4xx <string> (for general HTTP errors) or 5xx <string> (for Citrix-ADC-specific errors). The response payload provides details of the error.

- `Using REST APIs through SDKs`

  The following sample code specifies a VLAN for an admin partition.

`Java - Sample Code to specify the VLAN`

```
nspartition_vlan_binding nspartition_vlan_binding_object = new
nspartition_vlan_binding();



nspartition_vlan_binding_object.set_vlan(2);
```

```
nspartition_vlan_binding_object.set_partitionname("partition-dept1");



base_response result = nspartition_vlan_binding.add(nitroService,
nspartition_vlan_binding_object);
```

`.NET - Sample code to specify the VLAN`

```
nspartition_vlan_binding nspartition_vlan_binding_object = new
nspartition_vlan_binding();



nspartition_vlan_binding_object.vlan = 2;



nspartition_vlan_binding_object.partitionname = "partition-dept1";



base_response result = nspartition_vlan_binding.add(nitroService,
nspartition_vlan_binding_object);
```

`Python - Sample code to specify the VLAN`

```
nspartition_vlan_binding_object = nspartition_vlan_binding()



nspartition_vlan_binding_object.vlan = 2



nspartition_vlan_binding_object.partitionname = "partition-dept1"
```

```
result = nspartition_vlan_binding.add(nitroService,
nspartition_vlan_binding_object)
```

Switching Partitions

If you are associated with multiple admin partitions, you can switch to the required partition.

- `Using REST APIs through HTTP`

  The following example shows how to switch from current partition to a partition named partition-dept2.

- `Request`

  `HTTP Method:` POST

`URL:` http://<Citrix-ADC-IP-address(NSIP)>/nitro/v1/config/nspartition?action=Switch

`Request Headers:`

Cookie:NITRO_AUTH_TOKEN=<tokenvalue>

Content-Type:application/json

`Request Payload:`

```
{

    "nspartition":

    {

    "partitionname":"partition-dept2"

    }

}
```

- `Response`

  `HTTP Status Code on Success:` 201 Created

`HTTP Status Code on Failure:` 4xx <string> (for general HTTP errors) or 5xx <string> (for Citrix-ADC-specific errors). The response payload provides details of the error.

- `Using REST APIs through SDKs`

  The following sample code switches from current partition to a partition named "partition-dept2".

`Java - Sample code to switch partitions`

```
nspartition nspartitionObject = new nspartition();



vnspartitionObject.set_partitionname("partition-dept2");



base_response result = nspartition.Switch(nitroService,
nspartitionObject);
```

`.NET - Sample code to switch partitions`

```
nspartition nspartitionObject = new nspartition();



nspartitionObject.partitionname = "partition-dept2";



base_response result = nspartition.Switch(nitroService,
nspartitionObject);
```

`Python - Sample code to switch partitions`

```
nspartitionObject = nspartition()



nspartitionObject.partitionname = "partition-dept2"
```

```
result = nspartition.Switch(nitroService, nspartitionObject)
```

Managing AppExpert Applications

The following sections talks about exporting and importing an AppExpert application using NITRO APIs.

Exporting an AppExpert Application

This topic covers exporting an AppExpert application by using REST APIs through HTTP or SDKs.

- `Using REST APIs through HTTP`

  To export an AppExpert application, specify the parameters needed for the export operation in the apptemplateinfo object. Optionally, you can specify basic information about the AppExpert application template, such as the author of the configuration, a summary of the template functionality, and the template version number, in the template_info object. This information is stored as part of the template file that is created.

For example, to export an AppExpert application named MyApp1.

- `Request`

  `HTTP Method:` POST

`URL:` http://<Citrix-ADC-IP-address(NSIP)>/nitro/v1/config/apptemplateinfo?action=export

`Request Headers:`

Cookie:NITRO_AUTH_TOKEN=<tokenvalue>

Content-Type:application/json

`Request Payload:`

```
{

    "apptemplateinfo":

    {

        "appname":"MyApp1",
```

```
        "apptemplatefilename":"BizAp.xml",
        "template_info":
        {
            "templateversion_major":"2",
            "templateversion_minor":"1",
            "author":"XYZ",
            "introduction":"Intro",
            "summary":"Summary"
        }
    }
}
```

- `Response`

  `HTTP Status Code on Success:` 200 OK

`HTTP Status Code on Failure:` 4xx <string> (for general HTTP errors) or 5xx <string> (for Citrix-ADC-specific errors). The response payload provides details of the error.

- `Using REST APIs through SDKs`

  To export an AppExpert application, you must do the following:

1. Instantiate the com.citrix.netscaler.nitro.resource.config.app.application class.

   `Note.` For the python SDK, the package path is of the form nssrc.com.citrix.netscaler.....
2. Configure the properties of the AppExpert locally.
3. Export the AppExpert application.

The following samples export an AppExpert application named MyApp1.

`JAVA - sample code to export an AppExpert application`

```
application myapp = new application();

myapp.set_appname("MyApp1");

myapp.set_apptemplatefilename("myapp_template");

application.export(ns_session,myapp);
```

`.NET - sample code to export an AppExpert application`

```
application myapp = new application();

myapp.appname = "MyApp1";

myapp.apptemplatefilename = "myapp_template";

application.export(ns_session,myapp);
```

`Python - sample code to export an AppExpert application`

```
myapp = application()

myapp.appname = "MyApp1"

myapp.apptemplatefilename = "myapp_template"

application.export(ns_session, myapp)
```

Importing an AppExpert Application

This topic covers importing an AppExpert application by using REST APIs through HTTP or SDKs.

- `Using REST APIs through HTTP`

  To import an AppExpert application, specify the parameters needed for the import operation in the apptemplateinfo object.

For example, to import an AppExpert application named MyApp1.

- `Request`

  `HTTP Method:` POST

`URL:` http://<Citrix-ADC-IP-address(NSIP)>/nitro/v1/config/apptemplateinfo?action=import

`Request Headers:`

Cookie:NITRO_AUTH_TOKEN=<tokenvalue>

Content-Type:application/json

`Request Payload:`

```
{

"apptemplateinfo":

{

    "apptemplatefilename":"BizAp.xml",

    "deploymentfilename":"BizAp_deployment.xml",

    "appname":"MyApp1"

}

}
```

- `Response`

  `HTTP Status Code on Success:` 200 OK

`HTTP Status Code on Failure:` 4xx <string> (for general HTTP errors) or 5xx <string> (for Citrix-ADC-specific errors). The response payload provides details of the error.

To import an AppExpert application by specifying different deployment settings.

- `Request`

  `HTTP Method:` POST

`URL:` http://<Citrix-ADC-IP-address(NSIP)>/nitro/v1/config/apptemplateinfo?action=import

`Request Headers:`

Cookie:NITRO_AUTH_TOKEN=<tokenvalue>

Content-Type:application/json

`Request Payload:`

```
{

    "apptemplateinfo":

    {

    "apptemplatefilename":"BizAp.xml",

    "appname":"Myapp2",

    "deploymentinfo":

    {

        "appendpoint":

        [

            {

                "ipv46":"11.2.3.8",

                "port":80,

                "servicetype":"HTTP"

            }

        ],

        "service":

        [

            {

                "ip":"12.3.3.15",

                "port":80,
```

```
                "servicetype":"SSL"
            },
            {
                "ip":"14.5.5.16",
                "port":443,
                "servicetype":"SSL"
            }
        ]
    }
    }
}
```

- `Response`

  `HTTP Status Code on Success:` 200 OK

`HTTP Status Code on Failure:` 4xx <string> (for general HTTP errors) or 5xx <string> (for Citrix-ADC-specific errors). The response payload provides details of the error.

- `Using REST APIs through SDKs`

  To import an AppExpert application, you must do the following:

1. Instantiate the com.citrix.netscaler.nitro.resource.config.app.application class.

   `Note`. For the python SDK, the package path is of the form nssrc.com.citrix.netscaler.....
2. Configure the properties of the AppExpert locally.
3. Import the AppExpert application.

The following samples import an AppExpert application named MyApp1.

`Java - sample code to import an AppExpert application`

```
application myapp = new application();

myapp.set_appname("MyApp1");

myapp.set_apptemplatefilename("myapp_template");

application.Import(ns_session,myapp);
```

`.NET - sample code to import an AppExpert application`

```
application myapp = new application();

myapp.appname = "MyApp1";

myapp.apptemplatefilename = "myapp_template";

application.Import(ns_session,myapp);
```

`Python - sample code to import an AppExpert application`

```
myapp = application()

myapp.appname = "MyApp1"

myapp.apptemplatefilename = "myapp_template"

application.Import(ns_session, myapp)
```

Automate Citrix ADC Upgrade and Downgrade with a Single API

You can use the "install" API to automate not just installation, but also an upgrade or a downgrade of the build on a Citrix ADC appliance. You can specify a local or remote location for the build file.

- `Using REST APIs through HTTP`

  For example, the following information describes a downgrade to Citrix ADC release 10.5 build 46, using a local build file:

- `Request`

  `HTTP Method:` POST

`URL:` http://<NSIP\>/nitro/v1/config/install

`Request Headers:`

Cookie:NITRO_AUTH_TOKEN=\<tokenvalue \>

Content-Type: application/json

`Request Payload:`

```
{

“install”:

{

        “url”: “file:///var/tagma/build_tagma_46_nc.tgz”

    }

}
```

- `Response`

  `HTTP status Code on Success:`

201 Created

209 Citrix ADC specific warning

`Note.` when “y” option is not specified and warning is enabled, API returns “1120 - The configuration must be saved and the system rebooted for these settings to take effect” message in X-NITRO-WARNING.

`HTTP Status Code on Failure:` 599 Citrix ADC specific error

- `Additional parameters available in the install API request payload`
  - “y”:“true” - This option enables reboot on successful loading of kernel.
- “L”:“true” - This option enables the callhome feature.

`Supported formats for the "url" parameter (specifies the location of the tar.gz file for the build)`

- http://:@host/path/to/file
- https://:@host/path/to/file
- sftp://:@host/path/to/file
- scp://:@host/path/to/file
- ftp://:@host/path/to/file
- file://path/to/file
- `Possible errors`
  - Installation failed.
- Installation failed.
- Installation failed.
- Installation failed.
- Installation failed.
- Installation failed.
- Installation failed.
- Installation failed.

Handle Multiple NITRO Calls in a Single Request

You can use the "macroapi" API to create, update, and delete multiple resources simultaneously, and thereby minimize network traffic. For example, multiple load-balancing virtual servers can be added in a single API.

To account for the failure of some operations within the bulk operation, NITRO allows configuring one of the following behaviors.

- `EXIT`. When the first error is encountered, execution stops. The commands that were executed before the error are committed.
- `ROLLBACK`. When the first error is encountered, execution stops. The commands that were executed before the error are rolled back. Rollback is supported for add and bind commands only.
- `CONTINUE`. All the commands in the request are executed even if some commands fail.

You must specify the behavior of the bulk operation in the request header, by using the X-NITRO-ONERROR parameter.

- `Advantages`

  Heterogeneous resources can be configured with a single API. For example, multiple load balancing virtual servers and multiple services can be created, and services can be bound to load balancing virtual servers in a single API.

- `Limitations`

  Only homogenous operation is supported in this API. For example, multiple load balancing virtual servers can be created but cannot be updated or deleted in the same API. “rollback” is supported only on “add” and “bind” operations.

- `Using REST APIs through HTTP`

  To add multiple load balancing resources in a single request:

- `Request`

  `HTTP Method:` POST

`URL:` http://<NSIP\>/nitro/v1/config/macroapi

`Request Headers:`

Content-Type: application/json

Cookie: NITRO_AUTH_TOKEN=<tokenvalue>

X-NITRO-ONERROR: exit

`Request Payload:`

```
{

"lbvserver":[

{"name":"lbv1","servicetype":"http"},

{"name":"lbv2","servicetype":"http"}

],

"serviceGroup": [

{ "servicegroupname": "sg1", "servicetype": "HTTP" },

{ "servicegroupname": "sg2", "servicetype": "HTTP" }

],

"lbvserver_servicegroup_binding":[

{ "name":"lbv1", "servicegroupname":"sg1" },
```

```
{ "name":"lbv2", "servicegroupname":"sg2" }



]



}
```

- `Response`

  `HTTP Status Code on Success:` 201 Created for the add operation and 200 OK for the update operation.

`HTTP Status Code on Failure:` 207 Multi Status with error details in the response payload. For more information, see Error Handling.

For deleting multiple resources using macroapi, use POST HTTP method with query parameter “action=remove” in the URI.

Batch API support for NITRO calls

The `batchapi` API can handle multiple NITRO calls in a single request and thereby minimize network traffic.

You can perform the following operations using `batchapi`:

- You can use `batchapi` to create, update, and delete multiple `heterogenous` resources simultaneously.
- You can use `batchapi` to retrieve information of multiple heterogenous resources.

> `Note:`

> `batchapi` allows you to perform different operations across the NITRO resources in the request. Whereas `macroapi` limits to the same operation.

> To account for the failure of some operations within the bulk operation, NITRO allows configuring one of the following behaviors:

- `EXIT`. When the first error is encountered, execution stops. The commands that were executed before the error are committed.
- `CONTINUE`. All the commands in the request are executed even if some commands fail.

Ignore specific error messages for command by specifying list of error messages to be ignored as part of key `ignore_error_messages`.

Advantages of using Batch API

`batchapi` works like batch command in CLI, wherein you can perform multiple operations in a single API. For example, you can add multiple load balancing virtual servers, update multiple services, delete multiple services in a single API.

`batchapi` allows you to perform different operations across the NITRO resources in the request. Whereas the `macroapi` API limits to the same operation.

Limitations

- ROLLBACK on failure is not supported.
- `GET` operation cannot be executed along with the config operations.
- `batchapi` does not support the following operations:
  - `desiredState` API for servicegroup
  - `idempotent`
  - `bulkbindings`

Configure features using batch API

You can use `batchapi` to create, update, and delete multiple `heterogenous` resources simultaneously.

Use following convention to specify the action to be performed on each command within `batchapi`.

OPERATION TO PERFORM	ACTION KEY VALUE
CREATE/POST/BIND	ADD
UPDATE/PUT	SET
REMOVE/DELETE/UNBIND	REMOVE

Use the same keyword in the “action” field for non-CRUD operations. For example, enable, disable, link, unlink, and update operations.

The following `batchapi` request:

- enables load balancing feature
- adds a load balancing virtual server
- adds a servicegroup
- binds the load balancing virtual server to the servicegroup
- updates load balancing monitor response code in a single request

Request components

REQUEST FIELD	VALUE
HTTP Method	`POST`
URL	`http://<Citrix-ADC-IP-address(NSIP)>/nitro/v1/config/batchapi`
Request Headers	`Content-Type: application/json`
Request Payload	{"batchapi":[{"action": "disable", "type": "nsfeature", "properties": {"feature": }}, {"action": "ADD", "type": "lbvserver", "properties": {"name": "lbv1", "servicetype": "HTTP"}, "ignore_error_messages": {"errorcode" : 273, "message" : "Resource already exists"}]}, { "action": "ADD", "type": "servicegroup", "properties": {"servicegroupname": "sg1", "servicetype": "HTTP"}}, { "action": "ADD", "type": "lbvserver_servicegroup_binding", "properties": { "name": "lbv1", "servicegroupname": "sg1"}},

REQUEST FIELD	VALUE
	{ "action": "ADD", "type": "sslcertKey", "properties": {"certkey": "test_cert","cert": "ns-root.cert", "key": "ns-root.key"}}, { "action": "SET", "type": "lbmonitor", "properties": {"monitorname": "http", "type": "HTTP","respcode": }}]}

Response components

The following lists the possible status codes returned for a `batchapi` call used for configuring features:

- `HTTP Status Code on Success`: 201.
- `HTTP Status Code on Failure`: 207 Multi Status with error details in the response payload. For more information, see Error and Exception Handling.

Retrieve configuration information using batch API

You can use `batchapi` to retrieve information about multiple heterogenous resources.

> `Note:`
>
> Use either key `id` for sending unique identifier parameter value or use `properties` field to add unique identifier parameters (some resources have multiple unique identifier parameters).
>
> The following lists the query parameters that are supported in a `batchapi` show request:
>
> - `filter`. Retrieves filtered information.
> - `view`. Retrieves summarized information `view=summary`
> - `count`. Retrieves only the count of resources if `count=YES`
> - `attrs`. Retrieves information about the specified attributes.

Request components

The following request is an example to retrieve multiple resources in a single `batchapi` request.

REQUEST FIELD	VALUE
HTTP Method	`POST`
URL	`http://<Citrix-ADC-IP-address(NSIP)>/nitro/v1/config/batchapi?action=GET` or `http://<Citrix-ADC-IP-address(NSIP)>/nitro/v1/config/batchapi?action=SHOW`
Request Headers	`Content-Type: application/json`
Request Payload	{ "batchapi": [{ "type": "lbvserver", "id": "lbv1", "query_params" : {"attrs": } }, { "type": "lbvserver", "id": "lbv1", "query_params" : {"view": "summary"} }, { "type": "servicegroup", "query_params" : {"count": "YES"} }, { "type": "lbvserver_servicegroup_binding", "id": "lbv1", "query_params" : {"filter": {"servicegroupname": "sg1"}} }, { "type": "admparameter" }]}

Response components

The following lists the possible status codes returned for a `batchapi` call used for retrieving configuration information:

- `HTTP Status Code on Success`. 200 OK.
- `HTTP Status Code on Failure`. 207 Multi Status with error details in the response payload. For more information, see Error and Exception Handling.

The sample response payload contains the information that was requested:

RESPONSE FIELD	VALUE
Response payload	{ "batchapi" : [{ "errorcode" : 0, "lbvserver" : , "message" : "Done", "severity" : "NONE"},

RESPONSE FIELD	VALUE
	{ "errorcode" : 0, "lbvserver" : , "message" : "Done", "severity" : "NONE" }, { "errorcode" : 0, "message" : "Done", "servicegroup" : , "severity" : "NONE" }, {"errorcode" : 0, "lbvserver_servicegroup_binding" : , "message" : "Done", "severity" : "NONE" }, { "admparameter" : { "admserviceconnect" : "ENABLED" }, "errorcode" : 0, "message" : "Done", "severity" : "NONE" }], "errorcode" : 0, "message" : "Done", "severity" : "NONE" }

Update service group with desired member set seamlessly using Desired State API

One of the most frequently modified configurations on a Citrix ADC appliance is service group member set. Depending on the scale requirements or runtime changes to application servers, the service group member configuration on the appliance must be updated. In large scale and dynamically changing deployments, there might be a delay in updating the appliance configuration.

Desired State API solves this problem by accepting the intended member set for a service group in a single API, thereby effectively updating the configuration. Using Desired State API, you can:

- Provide a list of service group members in a single PUT request on “servicegroup_servicegroupmemberlist_binding” resource.
- Provide their weight and state (optional) in that PUT request.
- Effectively synchronize the appliance configuration with deployment changes around application servers.

The Citrix ADC appliance compares the requested desired member set with the configured member set. Then, it automatically binds the new members and unbinds the members that are not present in the request.

To enable graceful unbind of the service group members, set the `autodisablegraceful` and `autodisabledelay` parameters on the service group resource. When these parameters are set, the members are unbound gracefully as specified in the configuration and not immediately. For

more information on graceful unbind, see Configure a desired set of service group members for a service group in one NITRO API call.

Advantages of Desired State API

The following are some of the advantages of using the Desired State API.

- Better performance because a single API is used to bind and unbind multiple service group members.
  - Desired State API is better than macroapi for service group member changes, as one can perform only either bulk bind or bulk unbind but not both in single macroapi API.
  - Also, Desired State API implementation is driven inside the Citrix ADC Packet Engine which enhances performance.
- Synchronize deployment changes to Citrix ADC appliance in large scale deployments, such as Cloud Native deployments.

In large scale and highly dynamic deployments (for example Kubernetes, OpenShift, Pivotal), the challenge is to keep the appliance configuration up-to-date with the rate of change of deployments to accurately serve the application traffic.

In such deployments, controllers (Ingress or E-W Controller) are responsible for updating ADC configuration. In Kubernetes, whenever there are changes to deployment, kube-api server sends the effective set of endpoints through ‘Endpoints event’ to the controller. The controller uses the Read-Delta-Modify approach where it performs the following:

- Fetches the currently configured endpoint set (service group member set of a service group) for the service undergoing the change from ADC appliance.
- Compares the configured endpoint set with the set in the received event.
- Binds the new endpoints (service group members), or unbinds the deleted endpoints.

Because the rate of change and the size of services is high in this environment, this configuration method is not efficient and might delay configuration updates.

`Notes:`

- Support for Desired State API is available only for HA deployments.
- Support for Desired State API within macroapi is supported from release Citrix ADC 13.0 build 52.24.
- Desired State API within macroapi does not support rollback operation.

- The service group on which Desired State API is being used must have the Autoscale parameter set to “API.” Otherwise, Desired State NITRO API returns the “Operation not permitted” error.
- You can only bind IP address based services using Desired State API, Domain Name based services are not allowed.

Payloads

Request

`HTTP Method:` PUT `Request Headers:` Content-Type: application/json Cookie: NITRO_AUTH_TOKEN=`<tokenvalue>` URL: `http://<nsip>/nitro/v1/config/servicegroup_servicegroupmemberlist_binding/activesvcgrp`

`Request Payload:`

```
{

"servicegroup_servicegroupmemberlist_binding":

{

"servicegroupname":"activesvcgrp",

"members":

[

{ "ip":"10.112.123.17", "port":80, "weight":1},

{ "ip":"10.112.123.18", "port":8080, "weight":1},

{ "ip":"10.112.123.19", "port":80, "weight":1}

]

}

}
```

Response

`Success Case:`

`Headers:` HTTP/1.1 200 Ok `Payload:` NULL

`Failure Case` `Headers:` HTTP/1.1 207 Multi Status `Payload:` If there are validation failures, NITRO API returns an error with message indicating the problem with the request payload. For example,

```
{

"errorcode": 1110,

"message": "Invalid IP address [127.0.02]",

"severity": "ERROR"

}
```

If there are runtime failures (for example memory allocation failures), the ADC appliance might not be able to create all the desired member sets. In such cases, the NITRO API returns an error with `failedmembers` parameter listing the set of members which are not created. The recommendation is to retry the operation after some timeout. If the error persists, check the appliance memory and take action accordingly.

```
{

            “errorcode”:1442,

            “message”: “Failed to bind some servicegroup members”,

            “severity”: “ERROR”,

            “servicegroupmember_servicegroupmemberlist_binding”:

              {

                “servicegroupname”:”foo”,

                “failedmembers”:

                [

                              { "ip":"10.112.123.17", "port":8080,
```

```
"weight":1},

                                { "ip":"10.112.123.19", "port":80,
"weight":1}

                  ]

                }

}
```

Simplify Management Operations with an Idempotent API

You can add or update Citrix ADC resources seamlessly, with a single API. Previously, an attempt to add a resource that was already configured, or to update a resource that was not yet configured, caused an error.

If you enable the “idempotent” query parameter (“idempotent=yes”) in any POST request, NITRO executes the request in an idempotent manner. An idempotent HTTP method is an HTTP method that can be called many times without different results, and POST is desinged as a non-idempotent method.

`Note.` Use POST request with “idempotent” option if you are unsure whether the resource in the request exists on Citrix ADC or not.

This API hides the inconsistencies between parameter lists of POST and PUT operations. For some NITRO resources, certain parameters are accepted only on PUT not in POST, or vice versa. By using this idempotent API, you can overcome such challenges.

- `Limitations`

  If a resource is already configured and you try to add the same resource again, the resource is "updated," but the arguments already present are not unset. For example, if a load balancing virtual server named "V1" is configured to use the round robin load balancing method, and you try to ADD an lbvserver named "V1" without specifying a value for "lbmethod" in the request, the Citrix ADC appliance does not unset "lbmethod" to its default value of "leastconnection."

- `Using REST APIs through HTTP`

  In the following example, “preferredntpserver” is allowed only in PUT, but when given in POST request with idempotent=yes, NITRO internally adds the ntpserver and updates it with given properties.

- `Request`

  `HTTP Method:` POST

`URL:` http://<NSIP\>/nitro/v1/config/ntpserver?idempotent=yes

`Request Headers:`

Cookie:NITRO_AUTH_TOKEN=<tokenvalue>

Content-Type: application/json

`Request Payload:`

```
{



“ntpserver”:{“servername”:“ntp1”,“minpoll”:“4,  “preferredntpserver”:
“yes”}



}
```

- `Response`

  `HTTP Status Code on Success:` 200 OK

`HTTP Status Code on Failure:` 4xx <string> (for general HTTP errors) or 5xx <string> (for Citrix-ADC-specific errors). The response payload provides details of the error.

Retrieve Bindings in Bulk

This topic covers retrieving bindings information in bulk by using REST APIs through HTTP.

- `Using REST APIs through HTTP`

  You can use a bulk GET API to fetch bindings of all the entities of a given entity type.

For example, you can fetch bindings of all the load balancing virtual servers in one call instead of by using multiple GET by "name" calls. In the examples below, the Citrix ADC appliance has the following configuration.

- add lb vserver lbv1 http
- add lb vserver lbv2 http
- add service svc1 10.20.30.40 http 80
- add servicegroup sg1 http
- bind lb vserver lbv1 svc1
- bind lb vserver lbv1 sg1
- bind lb vserver lbv2 svc1
- bind lb vserver lbv2 sg1

`Example - To fetch bindings of all lbvservers, in a single NITRO API`

- `Request`

  `HTTP Method:` GET

`URL:` http://<NSIP\>/nitro/v1/config/lbvserver_binding?bulkbindings=yes

`Request Headers:`

Cookie:NITRO_AUTH_TOKEN=<tokenvalue>

Accept: application/json

- `Response`

  `HTTP Status Code on Success:` 200 OK

`HTTP Status Code on Failure:` 4xx <string> (for general HTTP errors) or 5xx <string> (for Citrix-ADC-specific errors). The response payload provides details of the error.

`Response Header:` Content-Type:application/json

`Response Payload:`

```
{



"errorcode":0,
```

```
"message":"Done",

"severity":"NONE",

"lbvserver_binding":[

{

    "name":"lbv1",

    "lbvserver_service_binding":[

    {

        "name":"lbv1",

        "servicename":"svc1",

        "stateflag":"536936451",

        "ipv46":"10.20.30.40",
```

```
        "port":80,

        "servicetype":"HTTP",

        "curstate":"DOWN",

        "weight":"1",

        "dynamicweight":"0",

        "cookieipport":"",

        "vserverid":"mcw1",

        "vsvrbindsvcip":"10.20.30.40",

        "vsvrbindsvcport":80,

        "preferredlocation":""

    }
```

```
    ],

    "lbvserver_servicegroup_binding":[

    {

        "name":"lbv1",

        "servicegroupname":"sg1",

        "stateflag":"536936464",

        "servicename":"sg1"

    }

    ]

},

{
```

```
    "name":"lbv2",

    "lbvserver_service_binding":[

    {

        "name":"lbv2",

        "servicename":"svc1",

        "stateflag":"536936451",

        "ipv46":"10.20.30.40",

        "port":80,

        "servicetype":"HTTP",

        "curstate":"DOWN",

        "weight":"1",
```

```
        "dynamicweight":"0",

        "cookieipport":"",

        "vserverid":"mcw2",

        "vsvrbindsvcip":"10.20.30.40",

        "vsvrbindsvcport":80,

        "preferredlocation":""

    }

    ],

    "lbvserver_servicegroup_binding":[

    {

        "name":"lbv2",
```

```
        "servicegroupname":"sg1",

        "stateflag":"536936464",

        "servicename":"sg1"

    }

    ]

}

]

}
```

`Example - To fetch only “service” bindings of all lbvservers`

- `Request`

  `HTTP Method:` GET

`URL:` http://<NSIP\>/nitro/v1/config/lbvserver_service_binding?bulkbindings=yes

`Request Header:` Content-Type:application/json

- `Response`

  `Response Payload:`

```
{

"errorcode":0,

"message":"Done",

"severity":"NONE",

"lbvserver_service_binding":[

    {

        "name":"lbv1",

        "servicename":"svc1",

        "stateflag":"536936451",

        "ipv46":"10.20.30.40",

        "port":80,
```

```
        "servicetype":"HTTP",

        "curstate":"DOWN",

        "weight":"1",

        "dynamicweight":"0",

        "cookieipport":"",

        "vserverid":"mcw1",

        "vsvrbindsvcip":"10.20.30.40",

        "vsvrbindsvcport":80,

        "preferredlocation":""

    },

    {
```

```
        "name":"lbv2",

        "servicename":"svc1",

        "stateflag":"536936451",

        "ipv46":"10.20.30.40",

        "port":80,

        "servicetype":"HTTP",

        "curstate":"DOWN",

        "weight":"1",

        "dynamicweight":"0",

        "cookieipport":"",

        "vserverid":"mcw2",
```

```
        "vsvrbindsvcip":"10.20.30.40",


        "vsvrbindsvcport":80,


        "preferredlocation":""


    }


    ]


}
```

View Individual Counter Information

This topic viewing individual counter information by using REST APIs through HTTP.

- `Using REST APIs through HTTP`

  To view global counters that are not otherwise shown by the Citrix ADC CLI or the GUI, you can now use the following URL format.

`URL`: http://<NSIP\>/nitro/v1/stat/nsglobalcntr?args=counters:\<counter1\>;\<counter2\>

Previously, these counter values could be viewed only through the “nsconmsg” Shell command.

`Note.` You can view only global counters of type ULONG and only up to 12 counters in a single request.

- `Example`

  This example shows how to view the individual counters http_tot_Requests and http_tot_Responses. Enter the details in the system or tool that you are using to generate HTTP or HTTPS requests.

- `Request`

  `HTTP Method:` GET

`URL:` http://<NSIP\>/nitro/v1/stat/nsglobalcntr?args=counters:http_tot_Requests;http_tot_Responses

- `Response`

```
{

"errorcode": 0,



"message": "Done",



"severity": "NONE",



"nsglobalcntr":

    {

    "http_tot_Requests": "5783",

    "http_tot_Responses": "5783"

    }

}
```

Prevent XSS and CSRF Attacks by Disabling Basic Authentication

As an administrator or a root user, you can now prevent users from making API calls after using basic authentication (such as one-time credentials) to log on. You can use this feature to prevent Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), and other types of attacks.

- `Procedure for Disabling Basic Authentication`

Use the following formats to enter the details in the system or tool that you are using to generate HTTP or HTTPS requests.

- `Using REST APIs through HTTP`
  - `Request`

    `URL:` http://<Citrix-ADC-ip-address(NSIP)\>/nitro/v1/config/systemparameter

`HTTP Method:` PUT

`Request Headers:`

Cookie:NITRO_AUTH_TOKEN=<tokenvalue>

Content-Type:application/json

`Request Payload:`

```
{

    "systemparameter":{ "basicauth":"disabled",}



}
```

- `Response`

  `HTTP Status Code on Success:` 200 OK

After you disable the basic authentication, access to Citrix ADC through the one-time password is denied and an error message is displayed.

- `Example`

  This example shows what happens if you make any API call after basic authentication has been disabled.

- `Request`

  `URL:` `<http://10.102.201.159/nitro/v1/config/lbvserver>`

`HTTP Method:` GET

After you make a GET call, the a logon screen appears. If you click `Log In` after entering the logon credentials, then you get the following response, which shows an error message.

- `Response`

```
{"errorcode": 1244,"message": "Authentication Failed: Use of Basic
Authentication is Disabled.","severity": "ERROR"

}
```

Error and Exception Handling

This section covers error handling support for NITRO APIs and exception handling support for SDKs.

Error Handling for NITRO APIs

In case of a failed request, NITRO provides the required information through the HTTP status code and in the response header and response payload.

- Error in a Single Resource Operation
- Error in a Bulk Operations
- Warnings
- `Error in a Single Resource Operation`

  The response of a single erroneous operation is as follows:
- `Response`

  `HTTP Status Code:` 4xx \<string\> (for general HTTP errors) or 5xx \<string\> (for Citrix-ADC-specific errors)

`Response Header:` Content-Type:application/json

`Response Payload:`

```
{

    errorcode: <Error code>,

    message: "<Error message>",

    severity: "ERROR"

}
```

- `Error in a Bulk Operation`

When there is a failure in one of the bulk operations, the response payload gives a combination of success and failure (depends on the value set for X-NITRO-ONERROR in the request header).

- `Response`

  `HTTP Status Code:` 207 Multi Status

`Response Header:` Content-Type:application/json

`Response Payload when X-NITRO-ONERROR is set to continue:`

When the first operation fails, the request is not terminated. The response payload shows the error details of the failed operation and the success status of the other operations.

```
{

    "errorcode": 1243,

    "message": "Bulk operation failed",

    "severity": "ERROR",

    "response":

    [

        {

            "errorcode": 273,

            "message": "Resource already exists",

            "severity": "ERROR"

        },

        {

            "errorcode": 0,

            "message": "Done",

            "severity": "NONE"
```

```
        }
    ]
}
```

`Response Payload when X-NITRO-ONERROR is set to exit:`

When the first operation fails, the request is terminated. The response payload only shows the error details of the failed operation.

```
{
    "errorcode": 1243,
    "message": "Bulk operation failed",
    "severity": "ERROR",
    "response":
    [
        {
            "errorcode": 273,
            "message": "Resource already exists",
            "severity": "ERROR"
        }
    ]
}
```

- `Warnings in NITRO Operations`

Warnings can be captured by specifying the "warning" query parameter as "yes" when performing any NITRO operation. For example, to get warnings while connecting to the Citrix ADC appliance, the URL is as follows:

http://<Citrix-ADC-IP-address(NSIP)>/nitro/v1/config/llbvserver?warning=yes

If there are any warnings, the response is as follows:

- `Response`

  `HTTP Status Code:` 209 X-NITRO-WARNING

`Response Header:` X-NITRO-WARNING →1067 - Feature(s) not enabled

Exception Handling Support for SDKs

The status of a NITRO request is captured in the com.citrix.netscaler.nitro.exception.nitro_exception class. This class provides the following details of the exception:

- `Session ID`. The session in which the exception occurred.
- `Severity`. The severity of the exception: error or warning. By default, only errors are captured. To capture warnings, you must set the warning flag to true, while connecting to the appliance.
- `Error code`. The status of the NITRO request. An error code of 0 indicates that the NITRO request is successful. A non-zero error code indicates an error in processing the NITRO request.
- `Error message`. Provides a brief description of the exception.

For a list of error codes, see the errorlisting.html file available in the \<NITRO_SDK_HOME\>/doc/api_reference folder.

API Reference

This documentation provides details of all operations that can be performed on the NetScaler appliance by using the REST API.

- Configuration
- Statistics
- Error Messages

Configuration

The configuration API is arranged in a logical groups of objects. Choose an appropriate group to find more details.

NAME	DESCRIPTION
AAA	Authentication, authorization, and accounting service configuration.
Adm	ADM related configuration.
Analytics	Analytics configuration.
Api	API Configuration
App	Application
Appflow	AppFlow configuration.
Application Firewall	Application Firewall configuration.

NAME	DESCRIPTION
Appqoe	Application Level Quality of Experience configuration
Audit	Audit configuration.
Authentication	Authentication configuration.
Authorization	Authorization configuration. Authorization services check which resources users are authorized to access, and grant permissions accordingly.
Autoscale	AutoScale configuration.
Azure	Azure configuration
Basic	Basic system configuration.
Bfd	Bidirectional Forwarding Detection
Bot	Bot Management.
Integrated Caching	Integrated Caching Configuration. The Integrated Caching feature is used to cache static and dynamic web application data.
Cloud	Citrix ADC as SD proxy Configuration and cloud discovery commands.
Cloudtunnel	Cloudtunnel Virtual server configuration.

NAME	DESCRIPTION
Cluster	Cluster commands.
Compression	Compression configuration. The system's feature for compressing HTTP responses to compression-aware browsers.
CI	Content Inspection
Cache Redirection	Cache redirection configuration. The cache redirection feature can transparently redirect cacheable HTTP requests to a cache and send non-cacheable or dynamic HTTP requests to the origin server. A cache stores or caches frequently requested web content and serves such web content to a client on behalf of the origin servers, alleviating the load on the origin server farm.
Content Switching	Content Switching configuration. Content Switching feature that enables you to direct traffic to servers on the basis of content.
Db	All the commands associated with database user
Denylist	Denylist level configuration.
Domain Name Service	Domain Name Service(DNS) configuration.
Dps	Citrix ADC DPS configuration.

NAME	DESCRIPTION
Endpoint	Lables attached to various endpoints
Front-end-optimization	Front end optimization configuration. The system's feature to optimize Web content for performance.
Global Server Load Balancing	Global Server Load Balancing (GSLB) configuration. GSLB feature ensures that client requests are directed to a best performing site available in a global enterprise and distributed Internet environment.
High Availability	High-availability commands.
Ica	ICA configuration.
Ipsec	IPSEC configuration.
Ipsecalg	IPSECALG configuration.
Kafka	Kafka Configuration
Load Balancing	Load Balancing configuration. The load balancing methods manage the selection of an appropriate physical server in a server farm.
LLDP	Link Layer Discovery Protocol.
Lsn	Large Scale NAT commands

NAME	DESCRIPTION
Metrics	Metrics configuration.
Network	Networking commands.
NS	System/Global level configuration.
NTP	NTP configuration.
Pcp	Port Control Protocol Configuration.
Policy	Policy configuration.
Protocol	Protocol Configuration.
Quic	QUIC configuration.
QuicBridge	QUIC Bridge configuration.
Rdp	RDP configuration.
Reputation	Reputation services configuration.
Responder	Responder configuration.
Rewrite	Rewrite configuration.
Router	Router configuration.
Smpp	All the commands associated with SMPP.

NAME	DESCRIPTION
SNMP	SNMP(Simple Network Management Protocol) configuration.
Spillover	Spillover policies and actions.
SSL	SSL Configuration
Stream	Stream configuration.
Subscriber	Subscriber configuration
System	System configuration.
Traffic Management	TM session/policy configuration.
Transform	URL Transformation configuration.
Tunnel	SSL VPN Tunnel Configuration.
Ulfd	ULFD server configuration.
User	User protocol configuration.
Utility	Utilities.
VideoOptimization	Video optimization feature is used to show (i) the stats of different media types that are being served by the Citrix ADC and (ii) the details of optimization applied on ABR videos

NAME	DESCRIPTION
SSL VPN	Virtual Private Network configuration.
Wasm	WASM Module configuration.

aaa

AAA

Authentication, authorization, and accounting service configuration.

NAME	DESCRIPTION
aaacertparams	Configuration for certificate parameter
aaaglobal_aaapreauthenticationpolicy_binding	Binding object showing the aaapreauthenticationpolicy that can be bound to aaaglobal
aaaglobal_authenticationnegotiateaction_binding	Binding object showing the authenticationnegotiateaction that can be bound to aaaglobal
aaaglobal_binding	Binding object showing the resources that can be bound to aaaglobal
aaagroup	Configuration for AAA group
aaagroup_aaauser_binding	Binding object showing the aaauser that can be bound to aaagroup
aaagroup_auditnslogpolicy_binding	Binding object showing the auditnslogpolicy that can be bound to aaagroup
aaagroup_auditsyslogpolicy_binding	Binding object showing the auditsyslogpolicy that can be bound to aaagroup

NAME	DESCRIPTION
aaagroup_authorizationpolicy_binding	Binding object showing the authorizationpolicy that can be bound to aaagroup
aaagroup_binding	Binding object showing the resources that can be bound to aaagroup
aaagroup_intranetip6_binding	Binding object showing the intranetip6 that can be bound to aaagroup
aaagroup_intranetip_binding	Binding object showing the intranetip that can be bound to aaagroup
aaagroup_tmsessionpolicy_binding	Binding object showing the tmsessionpolicy that can be bound to aaagroup
aaagroup_vpnintranetapplication_binding	Binding object showing the vpnintranetapplication that can be bound to aaagroup
aaagroup_vpnsecureprivateaccessprofile_binding	Binding object showing the vpnsecureprivateaccessprofile that can be bound to aaagroup
aaagroup_vpnsessionpolicy_binding	Binding object showing the vpnsessionpolicy that can be bound to aaagroup
aaagroup_vpntrafficpolicy_binding	Binding object showing the vpntrafficpolicy that can be bound to aaagroup
aaagroup_vpnurl_binding	Binding object showing the vpnurl that can be bound to aaagroup
aaagroup_vpnurlpolicy_binding	Binding object showing the vpnurlpolicy that can be bound to aaagroup

NAME	DESCRIPTION
aaakcdaccount	Configuration for Kerberos constrained delegation account
aaaldapparams	Configuration for LDAP parameter
aaaotpparameter	Configuration for AAA otpparameter
aaaparameter	Configuration for AAA parameter
aaapreauthenticationaction	Configuration for pre authentication action
aaapreauthenticationparameter	Configuration for pre authentication parameter
aaapreauthenticationpolicy	Configuration for pre authentication policy
aaapreauthenticationpolicy_aaaglobal_binding	Binding object showing the aaaglobal that can be bound to aaapreauthenticationpolicy
aaapreauthenticationpolicy_binding	Binding object showing the resources that can be bound to aaapreauthenticationpolicy
aaapreauthenticationpolicy_vpnvserver_binding	Binding object showing the vpnvserver that can be bound to aaapreauthenticationpolicy
aaaproxyparam	Configuration for AAA proxy parameter
aaaradiusparams	Configuration for RADIUS parameter
aaasession	Configuration for active connection
aaassoprofile	Configuration for aaa sso profile
aaatacacsparams	Configuration for tacacs parameters
aaauser	Configuration for AAA user
aaauser_aaagroup_binding	Binding object showing the aaagroup that can be bound to aaauser

NAME	DESCRIPTION
aaauser_auditnslogpolicy_binding	Binding object showing the auditnslogpolicy that can be bound to aaauser
aaauser_auditsyslogpolicy_binding	Binding object showing the auditsyslogpolicy that can be bound to aaauser
aaauser_authorizationpolicy_binding	Binding object showing the authorizationpolicy that can be bound to aaauser
aaauser_binding	Binding object showing the resources that can be bound to aaauser
aaauser_intranetip6_binding	Binding object showing the intranetip6 that can be bound to aaauser
aaauser_intranetip_binding	Binding object showing the intranetip that can be bound to aaauser
aaauser_tmsessionpolicy_binding	Binding object showing the tmsessionpolicy that can be bound to aaauser
aaauser_vpnintranetapplication_binding	Binding object showing the vpnintranetapplication that can be bound to aaauser
aaauser_vpnsecureprivateaccessprofile_binding	Binding object showing the vpnsecureprivateaccessprofile that can be bound to aaauser
aaauser_vpnsessionpolicy_binding	Binding object showing the vpnsessionpolicy that can be bound to aaauser
aaauser_vpntrafficpolicy_binding	Binding object showing the vpntrafficpolicy that can be bound to aaauser

NAME	DESCRIPTION
aaauser_vpnurl_binding	Binding object showing the vpnurl that can be bound to aaauser
aaauser_vpnurlpolicy_binding	Binding object showing the vpnurlpolicy that can be bound to aaauser

aaacertparams

Configuration for certificate parameter resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
usernamefield	<String>	Read-write	Client certificate field that contains the username, in the format <field>:<subfield>. .
groupnamefield	<String>	Read-write	Client certificate field that specifies the group, in the format <field>:<subfield>.
defaultauthentication group	<String>	Read-write	This is the default group that is chosen when the authentication succeeds in addition to extracted groups. Maximum length = 64
twofactor	<String>	Read-only	The state of the two-factor authentication. Possible values = ON, OFF

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- UPDATE
- UNSET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaacertparams **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"aaacertparams":{

"usernamefield":<String_value>,

"groupnamefield":<String_value>,

"defaultauthenticationgroup":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaacertparams? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"aaacertparams":{

"usernamefield":true,

"groupnamefield":true,

"defaultauthenticationgroup":true
```

```
}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaacertparams **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "aaacertparams": [ {

"twofactor":<String_value>,

"usernamefield":<String_value>,

"groupnamefield":<String_value>,

"defaultauthenticationgroup":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

aaaglobal_aaapreauthenticationpolicy_binding

Binding object showing the aaapreauthenticationpolicy that can be bound to aaaglobal.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
policy	<String>	Read-write	Name of the policy to be unbound. Minimum length = 1
priority	<Integer>	Read-write	Priority of the bound policy.
builtin	<String[]>	Read-write	Indicates that a variable is a built-in (SYSTEM INTERNAL) type. Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL
bindpolicytype	<Integer>	Read-only	Bound policy type.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/aaaglobal_aaapreauthenticationpolicy_binding
HTTP Method: PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"aaaglobal_aaapreauthenticationpolicy_binding":{

"policy":<String_value>,
```

```
"priority":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaaglobal_aaapreauthenticationpolicy_binding **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/aaaglobal_aaapreauthenticationpolicy_binding? **args=policy: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaaglobal_aaapreauthenticationpolicy_binding **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/aaaglobal_aaapreauthenticationpolicy_binding? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of aaaglobal_aaapreauthenticationpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/aaaglobal_aaapreauthenticationpolicy_binding? **pagesize=#no;pageno=#no**

Use this query-parameter to get the aaaglobal_aaapreauthenticationpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "aaaglobal_aaapreauthenticationpolicy_binding": [ {

"policy":<String_value>,

"priority":<Integer_value>,

"builtin":<String[]_value>,

"bindpolicytype":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/ aaaglobal_aaapreauthenticationpolicy_binding? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "aaaglobal_aaapreauthenticationpolicy_binding": [ { "__count":
"#no"} ] }
```

aaaglobal_authenticationnegotiateaction_binding

Binding object showing the authenticationnegotiateaction that can be bound to aaaglobal.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
windowsprofile	<String>	Read-write	Name of the negotiate profile to be bound. Minimum length = 1 Maximum length = 32
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/aaaglobal_authenticationnegotiateaction_binding
HTTP Method: PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"aaaglobal_authenticationnegotiateaction_binding":{

"windowsprofile":<String_value>
```

```
}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/ aaaglobal_authenticationnegotiateaction_binding **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/aaaglobal_authenticationnegotiateaction_binding? **args=windowsprofile: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/ aaaglobal_authenticationnegotiateaction_binding **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/aaaglobal_authenticationnegotiateaction_binding? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of aaaglobal_authenticationnegotiateaction_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ aaaglobal_authenticationnegotiateaction_binding? **pagesize=#no;pageno=#no**

Use this query-parameter to get the aaaglobal_authenticationnegotiateaction_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "aaaglobal_authenticationnegotiateaction_binding": [ {

"windowsprofile":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/ aaaglobal_authenticationnegotiateaction_binding? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "aaaglobal_authenticationnegotiateaction_binding": [ { "__count":
"#no"} ] }
```

aaaglobal_binding

Binding object which returns the resources bound to aaaglobal.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
aaaglobal_authenticationnegotiateaction_binding	<aaaglobal_authenticationnegotiateaction_binding[]>	Read-write	authenticationnegotiateaction that can be bound to aaaglobal.
aaaglobal_aaapreauthenticationpolicy_binding	<aaaglobal_aaapreauthenticationpolicy_binding[]>	Read-write	aaapreauthentication policy that can be bound to aaaglobal.

Operations

(click to see Properties)

- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaaglobal_binding

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "aaaglobal_binding": [ {

"aaaglobal_aaapreauthenticationpolicy_binding":<aaaglobal_aaapreauthentica
tionpolicy_binding[]_value>,

"aaaglobal_authenticationnegotiateaction_binding":<aaaglobal_authenticatio
nnegotiateaction_binding[]_value>
```

```
}]}
```

aaagroup

Configuration for AAA group resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
groupname	<String>	Read-write	Name for the group. Must begin with a letter, number, or the underscore character (_), and must consist only of letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore characters. Cannot be changed after the group is added. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			single quotation marks (for example, "my aaa group" or 'my aaa group'). Minimum length = 1
weight	<Integer>	Read-write	Weight of this group with respect to other configured aaa groups (lower the number higher the weight). Default value: 0 Minimum value = 0 Maximum value = 65535
loggedin	<Boolean>	Read-write	Display only the group members who are currently logged in. If there are large number of sessions, this command may provide partial details.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET (ALL)

- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaagroup **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"aaagroup":{

<b>"groupname":<String_value>,

</b>"weight":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaagroup/ groupname_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaagroup **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/aaagroup? **args=groupname: <String_value> ,loggedin: <Boolean_value>**

Use this query-parameter to get aaagroup resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/config/aaagroup? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/aaagroup? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of aaagroup resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/aaagroup? **view=summary**

Use this query-parameter to get the summary output of aaagroup resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/aaagroup? **pagesize=#no;pageno=#no**

Use this query-parameter to get the aaagroup resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "aaagroup": [ {

groupname:<String_value>,loggedin:<Boolean_value>"weight":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaagroup/ groupname_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/aaagroup/ groupname_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/aaagroup/ groupname_value<String> ? **view=summary**

Use this query-parameter to get the summary output of aaagroup resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "aaagroup": [ {

groupname:<String_value>,loggedin:<Boolean_value>"weight":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaagroup? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "aaagroup": [ { "__count": "#no"} ] }
```

aaagroup_aaauser_binding

Binding object showing the aaauser that can be bound to aaagroup.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
username	<String>	Read-write	The user name.
groupname	<String>	Read-write	Name of the group that you are binding. Minimum length = 1
gotopriorityexpression	<String>	Read-write	Expression or other value specifying the next policy to evaluate if the current policy evaluates to TRUE.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Specify one of the following values: * NEXT - Evaluate the policy with the next higher priority number. * END - End policy evaluation. * USE_INVOCATION_RESULT - Applicable if this policy invokes another policy label. If the final goto in the invoked policy label has a value of END, the evaluation stops. If the final goto is anything other than END, the current policy label performs a NEXT. * An expression that evaluates to a number. If you specify an expression, the number to which it evaluates determines the next policy to evaluate, as follows: * If the expression evaluates to a higher numbered priority, the policy with that priority is evaluated next. * If the expression evaluates to the priority of the current policy, the policy with the next higher numbered

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			priority is evaluated next. * If the expression evaluates to a number that is larger than the largest numbered priority, policy evaluation ends. An UNDEF event is triggered if: * The expression is invalid. * The expression evaluates to a priority number that is numerically lower than the current policy's priority. * The expression evaluates to a priority number that is between the current policy's priority number (say, 30) and the highest priority number (say, 100), but does not match any configured priority number (for example, the expression evaluates to the number 85). This example assumes that the priority number increments by 10 for every successive policy, and therefore a priority number of 85 does not exist in the policy label.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/aaagroup_aaauser_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"aaagroup_aaauser_binding":{

<b>"groupname":<String_value>,

</b>"username":<String_value>,

"gotopriorityexpression":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaagroup_aaauser_binding/ groupname_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ aaagroup_aaauser_binding/ groupname_value<String> ? **args=username: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaagroup_aaauser_binding/ groupname_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ aaagroup_aaauser_binding/ groupname_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of aaagroup_aaauser_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/aaagroup_aaauser_binding/ groupname_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the aaagroup_aaauser_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "aaagroup_aaauser_binding": [ {

"username":<String_value>,

"groupname":<String_value>,

"gotopriorityexpression":<String_value>
```

```
}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaagroup_aaauser_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/aaagroup_aaauser_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "aaagroup_aaauser_binding": [ {

"username":<String_value>,

"groupname":<String_value>,

"gotopriorityexpression":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaagroup_aaauser_binding/ groupname_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"aaagroup_aaauser_binding": [ { "__count": "#no"} ] }
```

aaagroup_auditnslogpolicy_binding

Binding object showing the auditnslogpolicy that can be bound to aaagroup.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
gotopriorityexpression	<String>	Read-write	Expression or other value specifying the next policy to evaluate if the current policy evaluates to TRUE. Specify one of the following values: * NEXT - Evaluate the policy with the next

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			higher priority number. * END - End policy evaluation. * USE_INVOCATION_RESULT - Applicable if this policy invokes another policy label. If the final goto in the invoked policy label has a value of END, the evaluation stops. If the final goto is anything other than END, the current policy label performs a NEXT. * An expression that evaluates to a number. If you specify an expression, the number to which it evaluates determines the next policy to evaluate, as follows: * If the expression evaluates to a higher numbered priority, the policy with that priority is evaluated next. * If the expression evaluates to the priority of the current policy, the policy with the next higher numbered priority is evaluated next. * If the expression evaluates to a number that is

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			larger than the largest numbered priority, policy evaluation ends. An UNDEF event is triggered if: * The expression is invalid. * The expression evaluates to a priority number that is numerically lower than the current policy's priority. * The expression evaluates to a priority number that is between the current policy's priority number (say, 30) and the highest priority number (say, 100), but does not match any configured priority number (for example, the expression evaluates to the number 85). This example assumes that the priority number increments by 10 for every successive policy, and therefore a priority number of 85 does not exist in the policy label.
policy	<String>	Read-write	The policy name.
type	<String>	Read-write	Bindpoint to which the policy is bound.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: REQUEST Possible values = REQUEST, UDP_REQUEST, DNS_REQUEST, ICMP_REQUEST
groupname	<String>	Read-write	Name of the group that you are binding. Minimum length = 1
priority	<Integer>	Read-write	Integer specifying the priority of the policy. A lower number indicates a higher priority. Policies are evaluated in the order of their priority numbers. Maximum value for default syntax policies is 2147483647 and for classic policies is 64000. Minimum value = 0 Maximum value = 2147483647
acttype	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD

- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/aaagroup_auditnslogpolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"aaagroup_auditnslogpolicy_binding":{

<b>"groupname":<String_value>,

</b>"policy":<String_value>,

"priority":<Integer_value>,

"type":<String_value>,

"gotopriorityexpression":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaagroup_auditnslogpolicy_binding/ groupname_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ aaagroup_auditnslogpolicy_binding/ groupname_value<String> ? **args=policy: <String_value> ,type: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaagroup_auditnslogpolicy_binding/ groupname_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ aaagroup_auditnslogpolicy_binding/ groupname_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of aaagroup_auditnslogpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/aaagroup_auditnslogpolicy_binding/ groupname_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the aaagroup_auditnslogpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "aaagroup_auditnslogpolicy_binding": [ {

"gotopriorityexpression":<String_value>,

"policy":<String_value>,

"type":<String_value>,

"groupname":<String_value>,

"priority":<Integer_value>,
```

```
"acttype":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaagroup_auditnslogpolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/aaagroup_auditnslogpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "aaagroup_auditnslogpolicy_binding": [ {

"gotopriorityexpression":<String_value>,

"policy":<String_value>,

"type":<String_value>,

"groupname":<String_value>,
```

```
"priority":<Integer_value>,

"acttype":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaagroup_auditnslogpolicy_binding/groupname_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"aaagroup_auditnslogpolicy_binding": [ { "__count": "#no"} ] }
```

aaagroup_auditsyslogpolicy_binding

Binding object showing the auditsyslogpolicy that can be bound to aaagroup.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
type	<String>	Read-write	Bindpoint to which the policy is bound.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: REQUEST Possible values = REQUEST, UDP_REQUEST, DNS_REQUEST, ICMP_REQUEST
groupname	<String>	Read-write	Name of the group that you are binding. Minimum length = 1
priority	<Integer>	Read-write	Integer specifying the priority of the policy. A lower number indicates a higher priority. Policies are evaluated in the order of their priority numbers. Maximum value for default syntax policies is 2147483647 and for classic policies is 64000. Minimum value = 0 Maximum value = 2147483647
gotopriorityexpression	<String>	Read-write	Expression or other value specifying the next policy to evaluate if the current policy evaluates to TRUE. Specify one of the following values: *

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			NEXT - Evaluate the policy with the next higher priority number. * END - End policy evaluation. * USE_INVOCATION_RESULT - Applicable if this policy invokes another policy label. If the final goto in the invoked policy label has a value of END, the evaluation stops. If the final goto is anything other than END, the current policy label performs a NEXT. * An expression that evaluates to a number. If you specify an expression, the number to which it evaluates determines the next policy to evaluate, as follows: * If the expression evaluates to a higher numbered priority, the policy with that priority is evaluated next. * If the expression evaluates to the priority of the current policy, the policy with the next higher numbered priority is evaluated next. * If the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			expression evaluates to a number that is larger than the largest numbered priority, policy evaluation ends. An UNDEF event is triggered if: * The expression is invalid. * The expression evaluates to a priority number that is numerically lower than the current policy's priority. * The expression evaluates to a priority number that is between the current policy's priority number (say, 30) and the highest priority number (say, 100), but does not match any configured priority number (for example, the expression evaluates to the number 85). This example assumes that the priority number increments by 10 for every successive policy, and therefore a priority number of 85 does not exist in the policy label.
policy	<String>	Read-write	The policy name.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
acttype	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/aaagroup_auditsyslogpolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"aaagroup_auditsyslogpolicy_binding":{

<b>"groupname":<String_value>,

</b>"policy":<String_value>,

"priority":<Integer_value>,

"type":<String_value>,

"gotopriorityexpression":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaagroup_auditsyslogpolicy_binding/ groupname_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ aaagroup_auditsyslogpolicy_binding/ groupname_value<String> ? **args=policy: <String_value> ,type: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaagroup_auditsyslogpolicy_binding/ groupname_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ aaagroup_auditsyslogpolicy_binding/ groupname_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of aaagroup_auditsyslogpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/aaagroup_auditsyslogpolicy_binding/ groupname_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the aaagroup_auditsyslogpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "aaagroup_auditsyslogpolicy_binding": [ {

"type":<String_value>,

"groupname":<String_value>,

"priority":<Integer_value>,

"gotopriorityexpression":<String_value>,

"policy":<String_value>,

"acttype":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaagroup_auditsyslogpolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/aaagroup_auditsyslogpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "aaagroup_auditsyslogpolicy_binding": [ {

"type":<String_value>,

"groupname":<String_value>,

"priority":<Integer_value>,

"gotopriorityexpression":<String_value>,

"policy":<String_value>,

"acttype":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaagroup_auditsyslogpolicy_binding/ groupname_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"aaagroup_auditsyslogpolicy_binding": [ { "__count": "#no"} ] }
```

aaagroup_authorizationpolicy_binding

Binding object showing the authorizationpolicy that can be bound to aaagroup.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
priority	<Integer>	Read-write	Integer specifying the priority of the policy. A lower number indicates a higher priority. Policies are evaluated in the order of their priority numbers. Maximum value for default syntax policies is 2147483647 and for classic policies is 64000. Minimum value = 0 Maximum value = 2147483647
groupname	<String>	Read-write	Name of the group that you are binding. Minimum length = 1
type	<String>	Read-write	Bindpoint to which the policy is bound. Default value: REQUEST Possible values = REQUEST, UDP_REQUEST, DNS_REQUEST, ICMP_REQUEST

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
policy	<String>	Read-write	The policy name.
gotopriorityexpression	<String>	Read-write	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
acttype	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/aaagroup_authorizationpolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"aaagroup_authorizationpolicy_binding":{

<b>"groupname":<String_value>,

</b>"policy":<String_value>,

"priority":<Integer_value>,

"type":<String_value>,

"gotopriorityexpression":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaagroup_authorizationpolicy_binding/ groupname_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ aaagroup_authorizationpolicy_binding/ groupname_value<String> ? **args=policy: <String_value> ,type: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaagroup_authorizationpolicy_binding/ groupname_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ aaagroup_authorizationpolicy_binding/ groupname_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of aaagroup_authorizationpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/aaagroup_authorizationpolicy_binding/ groupname_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the aaagroup_authorizationpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "aaagroup_authorizationpolicy_binding": [ {

"priority":<Integer_value>,

"groupname":<String_value>,

"type":<String_value>,

"policy":<String_value>,

"gotopriorityexpression":<String_value>,

"acttype":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaagroup_authorizationpolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/aaagroup_authorizationpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "aaagroup_authorizationpolicy_binding": [ {

"priority":<Integer_value>,

"groupname":<String_value>,

"type":<String_value>,

"policy":<String_value>,

"gotopriorityexpression":<String_value>,

"acttype":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaagroup_authorizationpolicy_binding/groupname_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"aaagroup_authorizationpolicy_binding": [ { "__count": "#no"} ] }
```

aaagroup_binding

Binding object which returns the resources bound to aaagroup.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
groupname	<String>	Read-write	Name of the group. Minimum length = 1
aaagroup_intranetip_binding	<aaagroup_intranetip_binding[]>	Read-only	intranetip that can be bound to aaagroup.
aaagroup_intranetip6_binding	<aaagroup_intranetip6_binding[]>	Read-only	intranetip6 that can be bound to aaagroup.
aaagroup_auditnslogpolicy_binding	<aaagroup_auditnslogpolicy_binding[]>	Read-only	auditnslogpolicy that can be bound to aaagroup.
aaagroup_aaauser_binding	<aaagroup_aaauser_binding[]>	Read-only	aaauser that can be bound to aaagroup.
aaagroup_vpnintranetapplication_binding	<aaagroup_vpnintranetapplication_binding[]>	Read-only	vpnintranetapplication that can be bound to aaagroup.
aaagroup_vpnsessionpolicy_binding	<aaagroup_vpnsessionpolicy_binding[]>	Read-only	vpnsessionpolicy that can be bound to aaagroup.
aaagroup_tmsessionpolicy_binding	<aaagroup_tmsessionpolicy_binding[]>	Read-only	tmsessionpolicy that can be bound to aaagroup.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
aaagroup_authorizationpolicy_binding	<aaagroup_authorizationpolicy_binding[]>	Read-only	authorizationpolicy that can be bound to aaagroup.
aaagroup_vpnsecureprivateaccessprofile_binding	<aaagroup_vpnsecureprivateaccessprofile_binding[]>	Read-only	vpnsecureprivateaccessprofile that can be bound to aaagroup.
aaagroup_auditsyslogpolicy_binding	<aaagroup_auditsyslogpolicy_binding[]>	Read-only	auditsyslogpolicy that can be bound to aaagroup.
aaagroup_vpntrafficpolicy_binding	<aaagroup_vpntrafficpolicy_binding[]>	Read-only	vpntrafficpolicy that can be bound to aaagroup.
aaagroup_vpnurlpolicy_binding	<aaagroup_vpnurlpolicy_binding[]>	Read-only	vpnurlpolicy that can be bound to aaagroup.
aaagroup_vpnurl_binding	<aaagroup_vpnurl_binding[]>	Read-only	vpnurl that can be bound to aaagroup.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaagroup_binding/ groupname_value<String>
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "aaagroup_binding": [ {

"groupname":<String_value>,

"aaagroup_intranetip6_binding":<aaagroup_intranetip6_binding[]_value>,
```

```
"aaagroup_vpnsecureprivateaccessprofile_binding":<aaagroup_vpnsecureprivat
eaccessprofile_binding[]_value>,

"aaagroup_tmsessionpolicy_binding":<aaagroup_tmsessionpolicy_binding[]_val
ue>,

"aaagroup_vpnintranetapplication_binding":<aaagroup_vpnintranetapplication
_binding[]_value>,

"aaagroup_intranetip_binding":<aaagroup_intranetip_binding[]_value>,

"aaagroup_vpnsessionpolicy_binding":<aaagroup_vpnsessionpolicy_binding[]_v
alue>,

"aaagroup_vpnurlpolicy_binding":<aaagroup_vpnurlpolicy_binding[]_value>,

"aaagroup_aaauser_binding":<aaagroup_aaauser_binding[]_value>,

"aaagroup_auditnslogpolicy_binding":<aaagroup_auditnslogpolicy_binding[]_v
alue>,

"aaagroup_vpnurl_binding":<aaagroup_vpnurl_binding[]_value>,

"aaagroup_auditsyslogpolicy_binding":<aaagroup_auditsyslogpolicy_binding[]
_value>,

"aaagroup_authorizationpolicy_binding":<aaagroup_authorizationpolicy_bindi
ng[]_value>,

"aaagroup_vpntrafficpolicy_binding":<aaagroup_vpntrafficpolicy_binding[]_v
alue>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaagroup_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ aaagroup_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "aaagroup_binding": [ {

"groupname":<String_value>,

"aaagroup_intranetip6_binding":<aaagroup_intranetip6_binding[]_value>,

"aaagroup_vpnsecureprivateaccessprofile_binding":<aaagroup_vpnsecureprivat
eaccessprofile_binding[]_value>,

"aaagroup_tmsessionpolicy_binding":<aaagroup_tmsessionpolicy_binding[]_val
ue>,

"aaagroup_vpnintranetapplication_binding":<aaagroup_vpnintranetapplication
_binding[]_value>,

"aaagroup_intranetip_binding":<aaagroup_intranetip_binding[]_value>,

"aaagroup_vpnsessionpolicy_binding":<aaagroup_vpnsessionpolicy_binding[]_v
alue>,

"aaagroup_vpnurlpolicy_binding":<aaagroup_vpnurlpolicy_binding[]_value>,

"aaagroup_aaauser_binding":<aaagroup_aaauser_binding[]_value>,
```

```
"aaagroup_auditnslogpolicy_binding":<aaagroup_auditnslogpolicy_binding[]_value>,

"aaagroup_vpnurl_binding":<aaagroup_vpnurl_binding[]_value>,

"aaagroup_auditsyslogpolicy_binding":<aaagroup_auditsyslogpolicy_binding[]_value>,

"aaagroup_authorizationpolicy_binding":<aaagroup_authorizationpolicy_binding[]_value>,

"aaagroup_vpntrafficpolicy_binding":<aaagroup_vpntrafficpolicy_binding[]_value>

}]}
```

aaagroup_intranetip6_binding

Binding object showing the intranetip6 that can be bound to aaagroup.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
intranetip6	<String>	Read-write	The Intranet IP6(s) bound to the group.
groupname	<String>	Read-write	Name of the group that you are binding. Minimum length = 1
numaddr	<Integer>	Read-write	Numbers of ipv6 address bound starting with intranetip6.
gotopriorityexpression	<String>	Read-write	Expression or other value specifying the next policy to evaluate if the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			current policy evaluates to TRUE. Specify one of the following values: * NEXT - Evaluate the policy with the next higher priority number. * END - End policy evaluation. * USE_INVOCATION_RESULT - Applicable if this policy invokes another policy label. If the final goto in the invoked policy label has a value of END, the evaluation stops. If the final goto is anything other than END, the current policy label performs a NEXT. * An expression that evaluates to a number. If you specify an expression, the number to which it evaluates determines the next policy to evaluate, as follows: * If the expression evaluates to a higher numbered priority, the policy with that priority is evaluated next. * If the expression evaluates to the priority of the current policy, the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			policy with the next higher numbered priority is evaluated next. * If the expression evaluates to a number that is larger than the largest numbered priority, policy evaluation ends. An UNDEF event is triggered if: * The expression is invalid. * The expression evaluates to a priority number that is numerically lower than the current policy's priority. * The expression evaluates to a priority number that is between the current policy's priority number (say, 30) and the highest priority number (say, 100), but does not match any configured priority number (for example, the expression evaluates to the number 85). This example assumes that the priority number increments by 10 for every successive policy, and therefore a priority number of

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			85 does not exist in the policy label.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/aaagroup_intranetip6_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"aaagroup_intranetip6_binding":{

<b>"groupname":<String_value>,

</b>"gotopriorityexpression":<String_value>,

"intranetip6":<String_value>,

"numaddr":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaagroup_intranetip6_binding/ groupname_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ aaagroup_intranetip6_binding/ groupname_value<String> ? **args=intranetip6: <String_value> ,numaddr: <Integer_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaagroup_intranetip6_binding/ groupname_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ aaagroup_intranetip6_binding/ groupname_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of aaagroup_intranetip6_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/aaagroup_intranetip6_binding/ groupname_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the aaagroup_intranetip6_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "aaagroup_intranetip6_binding": [ {

"intranetip6":<String_value>,
```

```
"groupname":<String_value>,

"numaddr":<Integer_value>,

"gotopriorityexpression":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaagroup_intranetip6_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/aaagroup_intranetip6_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "aaagroup_intranetip6_binding": [ {

"intranetip6":<String_value>,

"groupname":<String_value>,
```

```
"numaddr":<Integer_value>,

"gotopriorityexpression":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaagroup_intranetip6_binding/ groupname_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"aaagroup_intranetip6_binding": [ { "__count": "#no"} ] }
```

aaagroup_intranetip_binding

Binding object showing the intranetip that can be bound to aaagroup.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
netmask	<String>	Read-write	The netmask for the Intranet IP.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
groupname	<String>	Read-write	Name of the group that you are binding. Minimum length = 1
intranetip	<String>	Read-write	The Intranet IP(s) bound to the group.
gotopriorityexpression	<String>	Read-write	Expression or other value specifying the next policy to evaluate if the current policy evaluates to TRUE. Specify one of the following values: * NEXT - Evaluate the policy with the next higher priority number. * END - End policy evaluation. * USE_INVOCATION_RESULT - Applicable if this policy invokes another policy label. If the final goto in the invoked policy label has a value of END, the evaluation stops. If the final goto is anything other than END, the current policy label performs a NEXT. * An expression that evaluates to a number. If you specify an expression, the number to which it evaluates determines the next

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			policy to evaluate, as follows: * If the expression evaluates to a higher numbered priority, the policy with that priority is evaluated next. * If the expression evaluates to the priority of the current policy, the policy with the next higher numbered priority is evaluated next. * If the expression evaluates to a number that is larger than the largest numbered priority, policy evaluation ends. An UNDEF event is triggered if: * The expression is invalid. * The expression evaluates to a priority number that is numerically lower than the current policy's priority. * The expression evaluates to a priority number that is between the current policy's priority number (say, 30) and the highest priority number (say, 100), but does not match any configured priority number (for

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			example, the expression evaluates to the number 85). This example assumes that the priority number increments by 10 for every successive policy, and therefore a priority number of 85 does not exist in the policy label.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/aaagroup_intranetip_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"aaagroup_intranetip_binding":{

<b>"groupname":<String_value>,

</b>"intranetip":<String_value>,

"netmask":<String_value>,

"gotopriorityexpression":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaagroup_intranetip_binding/ groupname_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ aaagroup_intranetip_binding/ groupname_value<String> ? **args=intranetip: <String_value> ,netmask: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaagroup_intranetip_binding/ groupname_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ aaagroup_intranetip_binding/ groupname_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of aaagroup_intranetip_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/aaagroup_intranetip_binding/ groupname_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the aaagroup_intranetip_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "aaagroup_intranetip_binding": [ {

"netmask":<String_value>,

"groupname":<String_value>,

"intranetip":<String_value>,

"gotopriorityexpression":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaagroup_intranetip_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/aaagroup_intranetip_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "aaagroup_intranetip_binding": [ {

"netmask":<String_value>,

"groupname":<String_value>,

"intranetip":<String_value>,

"gotopriorityexpression":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaagroup_intranetip_binding/ groupname_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"aaagroup_intranetip_binding": [ { "__count": "#no"} ] }
```

aaagroup_tmsessionpolicy_binding

Binding object showing the tmsessionpolicy that can be bound to aaagroup.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
gotopriorityexpression	<String>	Read-write	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
policy	<String>	Read-write	The policy name.
type	<String>	Read-write	Bindpoint to which the policy is bound. Default value: REQUEST Possible values = REQUEST, UDP_REQUEST, DNS_REQUEST, ICMP_REQUEST
groupname	<String>	Read-write	Name of the group that you are binding. Minimum length = 1
priority	<Integer>	Read-write	Integer specifying the priority of the policy. A lower number indicates a higher priority. Policies are evaluated in the order of their priority numbers. Maximum value for default syntax policies is 2147483647 and for

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			classic policies is 64000. Minimum value = 0 Maximum value = 2147483647
acttype	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/aaagroup_tmsessionpolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"aaagroup_tmsessionpolicy_binding":{

<b>"groupname":<String_value>,

</b>"policy":<String_value>,

"priority":<Integer_value>,

"type":<String_value>,

"gotopriorityexpression":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaagroup_tmsessionpolicy_binding/ groupname_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ aaagroup_tmsessionpolicy_binding/ groupname_value<String> ? **args=policy: <String_value> ,type: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaagroup_tmsessionpolicy_binding/ groupname_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ aaagroup_tmsessionpolicy_binding/ groupname_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of aaagroup_tmsessionpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/aaagroup_tmsessionpolicy_binding/ groupname_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the aaagroup_tmsessionpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "aaagroup_tmsessionpolicy_binding": [ {

"gotopriorityexpression":<String_value>,

"policy":<String_value>,

"type":<String_value>,

"groupname":<String_value>,

"priority":<Integer_value>,

"acttype":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaagroup_tmsessionpolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/aaagroup_tmsessionpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "aaagroup_tmsessionpolicy_binding": [ {

"gotopriorityexpression":<String_value>,

"policy":<String_value>,

"type":<String_value>,

"groupname":<String_value>,

"priority":<Integer_value>,

"acttype":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaagroup_tmsessionpolicy_binding/ groupname_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"aaagroup_tmsessionpolicy_binding": [ { "__count": "#no"} ] }
```

aaagroup_vpnintranetapplication_binding

Binding object showing the vpnintranetapplication that can be bound to aaagroup.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
gotopriorityexpression	<String>	Read-write	Expression or other value specifying the next policy to evaluate if the current policy evaluates to TRUE. Specify one of the following values: * NEXT - Evaluate the policy with the next higher priority number. * END - End policy evaluation. * USE_INVOCATION_RESULT - Applicable if this policy invokes another policy label. If the final goto in the invoked policy label has a value of END, the evaluation stops. If the final goto is anything other than END, the current policy label performs a NEXT. * An expression that evaluates to a number. If you specify an

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			expression, the number to which it evaluates determines the next policy to evaluate, as follows: * If the expression evaluates to a higher numbered priority, the policy with that priority is evaluated next. * If the expression evaluates to the priority of the current policy, the policy with the next higher numbered priority is evaluated next. * If the expression evaluates to a number that is larger than the largest numbered priority, policy evaluation ends. An UNDEF event is triggered if: * The expression is invalid. * The expression evaluates to a priority number that is numerically lower than the current policy's priority. * The expression evaluates to a priority number that is between the current policy's priority number (say, 30) and the highest priority number (say,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			100), but does not match any configured priority number (for example, the expression evaluates to the number 85). This example assumes that the priority number increments by 10 for every successive policy, and therefore a priority number of 85 does not exist in the policy label.
intranetapplication	<String>	Read-write	Bind the group to the specified intranet VPN application.
groupname	<String>	Read-write	Name of the group that you are binding. Minimum length = 1
acttype	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/aaagroup_vpnintranetapplication_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"aaagroup_vpnintranetapplication_binding":{

<b>"groupname":<String_value>,
```

```
</b>"intranetapplication":<String_value>,

"gotopriorityexpression":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaagroup_vpnintranetapplication_binding/ groupname_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ aaagroup_vpnintranetapplication_binding/ groupname_value<String> ? **args=intranetapplication: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaagroup_vpnintranetapplication_binding/ groupname_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ aaagroup_vpnintranetapplication_binding/ groupname_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of aaagroup_vpnintranetapplication_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ aaagroup_vpnintranetapplication_binding/ groupname_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the aaagroup_vpnintranetapplication_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "aaagroup_vpnintranetapplication_binding": [ {

"gotopriorityexpression":<String_value>,

"intranetapplication":<String_value>,

"groupname":<String_value>,

"acttype":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaagroup_vpnintranetapplication_binding
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/aaagroup_vpnintranetapplication_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "aaagroup_vpnintranetapplication_binding": [ {

"gotopriorityexpression":<String_value>,

"intranetapplication":<String_value>,

"groupname":<String_value>,

"acttype":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaagroup_vpnintranetapplication_binding/groupname_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"aaagroup_vpnintranetapplication_binding": [ { "__count": "#no"} ] }
```

aaagroup_vpnsecureprivateaccessprofile_binding

Binding object showing the vpnsecureprivateaccessprofile that can be bound to aaagroup.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
groupname	<String>	Read-write	Name of the group that you are binding. Minimum length = 1
secureprivateaccess profile	<String>	Read-write	Name of the Secure Private Access Profile bound to the group.
gotopriorityexpressio n	<String>	Read-write	Expression or other value specifying the next policy to evaluate if the current policy evaluates to TRUE. Specify one of the following values: * NEXT - Evaluate the policy with the next higher priority number. * END - End policy evaluation. *

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			USE_INVOCATION_RESULT - Applicable if this policy invokes another policy label. If the final goto in the invoked policy label has a value of END, the evaluation stops. If the final goto is anything other than END, the current policy label performs a NEXT. * An expression that evaluates to a number. If you specify an expression, the number to which it evaluates determines the next policy to evaluate, as follows: * If the expression evaluates to a higher numbered priority, the policy with that priority is evaluated next. * If the expression evaluates to the priority of the current policy, the policy with the next higher numbered priority is evaluated next. * If the expression evaluates to a number that is larger than the largest numbered priority, policy

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			evaluation ends. An UNDEF event is triggered if: * The expression is invalid. * The expression evaluates to a priority number that is numerically lower than the current policy's priority. * The expression evaluates to a priority number that is between the current policy's priority number (say, 30) and the highest priority number (say, 100), but does not match any configured priority number (for example, the expression evaluates to the number 85). This example assumes that the priority number increments by 10 for every successive policy, and therefore a priority number of 85 does not exist in the policy label.
acttype	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/ aaagroup_vpnsecureprivateaccessprofile_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"aaagroup_vpnsecureprivateaccessprofile_binding":{

<b>"groupname":<String_value>,

</b>"gotopriorityexpression":<String_value>,

"secureprivateaccessprofile":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/ aaagroup_vpnsecureprivateaccessprofile_binding/ groupname_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ aaagroup_vpnsecureprivateaccessprofile_binding/ groupname_value<String> ? **args=secureprivateaccessprofile: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/ aaagroup_vpnsecureprivateaccessprofile_binding/ groupname_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ aaagroup_vpnsecureprivateaccessprofile_binding/ groupname_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of aaagroup_vpnsecureprivateaccessprofile_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ aaagroup_vpnsecureprivateaccessprofile_binding/ groupname_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the aaagroup_vpnsecureprivateaccessprofile_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "aaagroup_vpnsecureprivateaccessprofile_binding": [ {

"groupname":<String_value>,

"secureprivateaccessprofile":<String_value>,
```

```
"gotopriorityexpression":<String_value>,

"acttype":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/ aaagroup_vpnsecureprivateaccessprofile_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ aaagroup_vpnsecureprivateaccessprofile_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "aaagroup_vpnsecureprivateaccessprofile_binding": [ {

"groupname":<String_value>,

"secureprivateaccessprofile":<String_value>,

"gotopriorityexpression":<String_value>,
```

```
"acttype":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/ aaagroup_vpnsecureprivateaccessprofile_binding/ groupname_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"aaagroup_vpnsecureprivateaccessprofile_binding": [ { "__count":
"#no"} ] }
```

aaagroup_vpnsessionpolicy_binding

Binding object showing the vpnsessionpolicy that can be bound to aaagroup.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
policy	<String>	Read-write	The policy name.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
gotopriorityexpression	<String>	Read-write	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
priority	<Integer>	Read-write	Integer specifying the priority of the policy. A lower number indicates a higher priority. Policies are evaluated in the order of their priority numbers. Maximum value for default syntax policies is 2147483647 and for classic policies is 64000. Minimum value = 0 Maximum value = 2147483647
groupname	<String>	Read-write	Name of the group that you are binding. Minimum length = 1
type	<String>	Read-write	Bindpoint to which the policy is bound. Default value: REQUEST Possible values = REQUEST, UDP_REQUEST,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			DNS_REQUEST, ICMP_REQUEST
acttype	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/aaagroup_vpnsessionpolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"aaagroup_vpnsessionpolicy_binding":{

<b>"groupname":<String_value>,

</b>"policy":<String_value>,

"priority":<Integer_value>,

"type":<String_value>,

"gotopriorityexpression":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaagroup_vpnsessionpolicy_binding/groupname_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/

aaagroup_vpnsessionpolicy_binding/ groupname_value<String> ? **args=policy: <String_value> ,type: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaagroup_vpnsessionpolicy_binding/ groupname_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ aaagroup_vpnsessionpolicy_binding/ groupname_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of aaagroup_vpnsessionpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/aaagroup_vpnsessionpolicy_binding/ groupname_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the aaagroup_vpnsessionpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "aaagroup_vpnsessionpolicy_binding": [ {

"policy":<String_value>,

"gotopriorityexpression":<String_value>,

"priority":<Integer_value>,

"groupname":<String_value>,

"type":<String_value>,

"acttype":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaagroup_vpnsessionpolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/aaagroup_vpnsessionpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "aaagroup_vpnsessionpolicy_binding": [ {

"policy":<String_value>,

"gotopriorityexpression":<String_value>,

"priority":<Integer_value>,

"groupname":<String_value>,

"type":<String_value>,

"acttype":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaagroup_vpnsessionpolicy_binding/ groupname_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"aaagroup_vpnsessionpolicy_binding": [ { "__count": "#no"} ] }
```

aaagroup_vpntrafficpolicy_binding

Binding object showing the vpntrafficpolicy that can be bound to aaagroup.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
type	<String>	Read-write	Bindpoint to which the policy is bound. Default value: REQUEST Possible values = REQUEST, UDP_REQUEST, DNS_REQUEST, ICMP_REQUEST
groupname	<String>	Read-write	Name of the group that you are binding. Minimum length = 1
priority	<Integer>	Read-write	Integer specifying the priority of the policy. A lower number indicates a higher priority. Policies are evaluated in the order of their priority numbers. Maximum value for default syntax policies is 2147483647 and for classic policies is 64000. Minimum value = 0 Maximum value = 2147483647

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
gotopriorityexpression	<String>	Read-write	Expression or other value specifying the next policy to evaluate if the current policy evaluates to TRUE. Specify one of the following values: * NEXT - Evaluate the policy with the next higher priority number. * END - End policy evaluation. * USE_INVOCATION_RESULT - Applicable if this policy invokes another policy label. If the final goto in the invoked policy label has a value of END, the evaluation stops. If the final goto is anything other than END, the current policy label performs a NEXT. * An expression that evaluates to a number. If you specify an expression, the number to which it evaluates determines the next policy to evaluate, as follows: * If the expression evaluates to a higher numbered priority, the policy with that priority is evaluated

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			next. * If the expression evaluates to the priority of the current policy, the policy with the next higher numbered priority is evaluated next. * If the expression evaluates to a number that is larger than the largest numbered priority, policy evaluation ends. An UNDEF event is triggered if: * The expression is invalid. * The expression evaluates to a priority number that is numerically lower than the current policy's priority. * The expression evaluates to a priority number that is between the current policy's priority number (say, 30) and the highest priority number (say, 100), but does not match any configured priority number (for example, the expression evaluates to the number 85). This example assumes that the priority number increments by 10 for

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			every successive policy, and therefore a priority number of 85 does not exist in the policy label.
policy	<String>	Read-write	The policy name.
acttype	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/aaagroup_vpntrafficpolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"aaagroup_vpntrafficpolicy_binding":{

<b>"groupname":<String_value>,

</b>"policy":<String_value>,

"priority":<Integer_value>,

"type":<String_value>,

"gotopriorityexpression":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaagroup_vpntrafficpolicy_binding/ groupname_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ aaagroup_vpntrafficpolicy_binding/ groupname_value<String> ? **args=policy: <String_value> ,type: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaagroup_vpntrafficpolicy_binding/ groupname_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ aaagroup_vpntrafficpolicy_binding/ groupname_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of aaagroup_vpntrafficpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/aaagroup_vpntrafficpolicy_binding/ groupname_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the aaagroup_vpntrafficpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "aaagroup_vpntrafficpolicy_binding": [ {

"type":<String_value>,

"groupname":<String_value>,

"priority":<Integer_value>,

"gotopriorityexpression":<String_value>,

"policy":<String_value>,

"acttype":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaagroup_vpntrafficpolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/aaagroup_vpntrafficpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "aaagroup_vpntrafficpolicy_binding": [ {

"type":<String_value>,

"groupname":<String_value>,

"priority":<Integer_value>,

"gotopriorityexpression":<String_value>,

"policy":<String_value>,

"acttype":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaagroup_vpntrafficpolicy_binding/ groupname_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"aaagroup_vpntrafficpolicy_binding": [ { "__count": "#no"} ] }
```

aaagroup_vpnurl_binding

Binding object showing the vpnurl that can be bound to aaagroup.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
gotopriorityexpression	<String>	Read-write	Expression or other value specifying the next policy to evaluate if the current policy evaluates to TRUE. Specify one of the following values: * NEXT - Evaluate the policy with the next higher priority number. * END - End policy evaluation. * USE_INVOCATION_RESULT - Applicable if this policy invokes another policy label. If the final goto in the invoked policy label has a value of END, the evaluation stops. If the final goto is anything other than END, the current policy label performs a NEXT. * An expression that evaluates to a number. If you specify an

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			expression, the number to which it evaluates determines the next policy to evaluate, as follows: * If the expression evaluates to a higher numbered priority, the policy with that priority is evaluated next. * If the expression evaluates to the priority of the current policy, the policy with the next higher numbered priority is evaluated next. * If the expression evaluates to a number that is larger than the largest numbered priority, policy evaluation ends. An UNDEF event is triggered if: * The expression is invalid. * The expression evaluates to a priority number that is numerically lower than the current policy's priority. * The expression evaluates to a priority number that is between the current policy's priority number (say, 30) and the highest priority number (say,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			100), but does not match any configured priority number (for example, the expression evaluates to the number 85). This example assumes that the priority number increments by 10 for every successive policy, and therefore a priority number of 85 does not exist in the policy label.
urlname	<String>	Read-write	The intranet url.
groupname	<String>	Read-write	Name of the group that you are binding. Minimum length = 1
acttype	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/aaagroup_vpnurl_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"aaagroup_vpnurl_binding":{

<b>"groupname":<String_value>,

</b>"urlname":<String_value>,
```

```
"gotopriorityexpression":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaagroup_vpnurl_binding/ groupname_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ aaagroup_vpnurl_binding/ groupname_value<String> ? **args=urlname: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaagroup_vpnurl_binding/ groupname_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ aaagroup_vpnurl_binding/ groupname_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of aaagroup_vpnurl_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/aaagroup_vpnurl_binding/ groupname_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the aaagroup_vpnurl_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "aaagroup_vpnurl_binding": [ {

"gotopriorityexpression":<String_value>,

"urlname":<String_value>,

"groupname":<String_value>,

"acttype":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaagroup_vpnurl_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/aaagroup_vpnurl_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "aaagroup_vpnurl_binding": [ {

"gotopriorityexpression":<String_value>,

"urlname":<String_value>,

"groupname":<String_value>,

"acttype":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaagroup_vpnurl_binding/ groupname_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"aaagroup_vpnurl_binding": [ { "__count": "#no"} ] }
```

aaagroup_vpnurlpolicy_binding

Binding object showing the vpnurlpolicy that can be bound to aaagroup.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
groupname	<String>	Read-write	Name of the group that you are binding. Minimum length = 1
priority	<Integer>	Read-write	Integer specifying the priority of the policy. A lower number indicates a higher priority. Policies are evaluated in the order of their priority numbers. Maximum value for default syntax policies is 2147483647 and for classic policies is 64000. Minimum value = 0 Maximum value = 2147483647
type	<String>	Read-write	Bindpoint to which the policy is bound. Default value: REQUEST

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = REQUEST, UDP_REQUEST, DNS_REQUEST, ICMP_REQUEST
policy	<String>	Read-write	The policy name.
gotopriorityexpression	<String>	Read-write	Expression or other value specifying the next policy to evaluate if the current policy evaluates to TRUE. Specify one of the following values: * NEXT - Evaluate the policy with the next higher priority number. * END - End policy evaluation. * USE_INVOCATION_RESULT - Applicable if this policy invokes another policy label. If the final goto in the invoked policy label has a value of END, the evaluation stops. If the final goto is anything other than END, the current policy label performs a NEXT. * An expression that evaluates to a number. If you specify an expression, the number to which it evaluates

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			determines the next policy to evaluate, as follows: * If the expression evaluates to a higher numbered priority, the policy with that priority is evaluated next. * If the expression evaluates to the priority of the current policy, the policy with the next higher numbered priority is evaluated next. * If the expression evaluates to a number that is larger than the largest numbered priority, policy evaluation ends. An UNDEF event is triggered if: * The expression is invalid. * The expression evaluates to a priority number that is numerically lower than the current policy's priority. * The expression evaluates to a priority number that is between the current policy's priority number (say, 30) and the highest priority number (say, 100), but does not match any configured priority

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			number (for example, the expression evaluates to the number 85). This example assumes that the priority number increments by 10 for every successive policy, and therefore a priority number of 85 does not exist in the policy label.
acttype	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/aaagroup_vpnurlpolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"aaagroup_vpnurlpolicy_binding":{

<b>"groupname":<String_value>,

</b>"policy":<String_value>,

"priority":<Integer_value>,

"type":<String_value>,

"gotopriorityexpression":<String_value>
```

```
}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaagroup_vpnurlpolicy_binding/ groupname_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/aaagroup_vpnurlpolicy_binding/ groupname_value<String> ? **args=policy: <String_value> ,type: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaagroup_vpnurlpolicy_binding/ groupname_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/aaagroup_vpnurlpolicy_binding/ groupname_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of aaagroup_vpnurlpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/aaagroup_vpnurlpolicy_binding/ groupname_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the aaagroup_vpnurlpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "aaagroup_vpnurlpolicy_binding": [ {

"groupname":<String_value>,

"priority":<Integer_value>,

"type":<String_value>,

"policy":<String_value>,

"gotopriorityexpression":<String_value>,

"acttype":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaagroup_vpnurlpolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/aaagroup_vpnurlpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "aaagroup_vpnurlpolicy_binding": [ {

"groupname":<String_value>,

"priority":<Integer_value>,

"type":<String_value>,

"policy":<String_value>,

"gotopriorityexpression":<String_value>,

"acttype":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaagroup_vpnurlpolicy_binding/ groupname_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"aaagroup_vpnurlpolicy_binding": [ { "__count": "#no"} ] }
```

aaakcdaccount

Configuration for Kerberos constrained delegation account resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
kcdaccount	<String>	Read-write	The name of the KCD account. Minimum length = 1
keytab	<String>	Read-write	The path to the keytab file. If specified other parameters in this command need not be given.
realmstr	<String>	Read-write	Kerberos Realm.
delegateduser	<String>	Read-write	Username that can perform kerberos constrained delegation.
kcdpassword	<String>	Read-write	Password for Delegated User.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
usercert	<String>	Read-write	SSL Cert (including private key) for Delegated User.
cacert	<String>	Read-write	CA Cert for UserCert or when doing PKINIT backchannel.
userrealm	<String>	Read-write	Realm of the user.
enterpriserealm	<String>	Read-write	Enterprise Realm of the user. This should be given only in certain KDC deployments where KDC expects Enterprise username instead of Principal Name.
servicespn	<String>	Read-write	Service SPN. When specified, this will be used to fetch kerberos tickets. If not specified, Citrix ADC will construct SPN using service fqdn.
saltexpression	<String>	Read-write	Salt expression used by Kerberos impersonation. When configured, this expression will be used for key derivation with AES-128 or AES-256 encryption types. For RC4

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			encryption, the salt is not used. If the salt expression is not set, the default behavior is to derive the salt value from the Kerberos principal.
principle	<String>	Read-only	SPN extracted from keytab file.
kcdspn	<String>	Read-only	Host SPN extracted from keytab file.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT
- CHECK

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaakcdaccount **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"aaakcdaccount":{

<b>"kcdaccount":<String_value>,

</b>"keytab":<String_value>,

"realmstr":<String_value>,
```

```
"delegateduser":<String_value>,

"kcdpassword":<String_value>,

"usercert":<String_value>,

"cacert":<String_value>,

"userrealm":<String_value>,

"enterpriserealm":<String_value>,

"servicespn":<String_value>,

"saltexpression":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaakcdaccount/ kcdaccount_value<String>
HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaakcdaccount **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"aaakcdaccount":{

<b>"kcdaccount":<String_value>,

</b>"keytab":<String_value>,

"realmstr":<String_value>,

"delegateduser":<String_value>,

"kcdpassword":<String_value>,

"usercert":<String_value>,

"cacert":<String_value>,

"userrealm":<String_value>,

"enterpriserealm":<String_value>,

"servicespn":<String_value>,

"saltexpression":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaakcdaccount? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"aaakcdaccount":{

<b>"kcdaccount":<String_value>,

</b>"keytab":true,

"usercert":true,

"cacert":true,

"userrealm":true,

"enterpriserealm":true,

"servicespn":true,

"saltexpression":true,

"delegateduser":true,

"kcdpassword":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

CHECK

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaakcdaccount? **action=check HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"aaakcdaccount":{

<b>"realmstr":<String_value>,

</b><b>"delegateduser":<String_value>,

</b><b>"kcdpassword":<String_value>,

</b><b>"servicespn":<String_value>,

</b>"userrealm":<String_value>,

"saltexpression":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Payload:

```
{ "aaakcdaccount": [ {



}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaakcdaccount **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/aaakcdaccount? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/aaakcdaccount? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of aaakcdaccount resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/aaakcdaccount? **view=summary**

Use this query-parameter to get the summary output of aaakcdaccount resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/aaakcdaccount? **pagesize=#no;pageno=#no**

Use this query-parameter to get the aaakcdaccount resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "aaakcdaccount": [ {

"kcdaccount":<String_value>,

"keytab":<String_value>,

"principle":<String_value>,

"kcdspn":<String_value>,

"realmstr":<String_value>,
```

```
"delegateduser":<String_value>,

"kcdpassword":<String_value>,

"usercert":<String_value>,

"cacert":<String_value>,

"userrealm":<String_value>,

"enterpriserealm":<String_value>,

"servicespn":<String_value>,

"saltexpression":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaakcdaccount/ kcdaccount_value<String>
Query-parameters: attrs http:// <netscaler-ip-address> /nitro/v1/config/aaakcdaccount/ kcdaccount_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/aaakcdaccount/ kcdaccount_value<String> ? **view=summary**

Use this query-parameter to get the summary output of aaakcdaccount resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "aaakcdaccount": [ {

"kcdaccount":<String_value>,

"keytab":<String_value>,

"principle":<String_value>,

"kcdspn":<String_value>,

"realmstr":<String_value>,

"delegateduser":<String_value>,

"kcdpassword":<String_value>,

"usercert":<String_value>,

"cacert":<String_value>,

"userrealm":<String_value>,

"enterpriserealm":<String_value>,

"servicespn":<String_value>,

"saltexpression":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

```
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaakcdaccount? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "aaakcdaccount": [ { "__count": "#no"} ] }
```

aaaldapparams

Configuration for LDAP parameter resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
serverip	<String>	Read-write	IP address of your LDAP server.
serverport	<Integer>	Read-write	Port number on which the LDAP server listens for connections.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: 389 Minimum value = 1
authtimeout	<Integer>	Read-write	Maximum number of seconds that the Citrix ADC waits for a response from the LDAP server. Default value: 3 Minimum value = 1
ldapbase	<String>	Read-write	Base (the server and location) from which LDAP search commands should start. If the LDAP server is running locally, the default value of base is dc=netscaler, dc=com.
ldapbinddn	<String>	Read-write	Complete distinguished name (DN) string used for binding to the LDAP server.
ldapbinddnpassword	<String>	Read-write	Password for binding to the LDAP server. Minimum length = 1
ldaploginname	<String>	Read-write	Name attribute that the Citrix ADC uses to query the external LDAP server or an Active Directory.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
searchfilter	<String>	Read-write	String to be combined with the default LDAP user search string to form the value to use when executing an LDAP search. For example, the following values: vpnallowed=true, ldaploginame=""samaccount"" when combined with the user-supplied username ""bob"", yield the following LDAP search string: ""(;(vpnallowed=true)(samaccount=bob)"" . Minimum length = 1
groupattrname	<String>	Read-write	Attribute name used for group extraction from the LDAP server.
subattributename	<String>	Read-write	Subattribute name used for group extraction from the LDAP server.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
sectype	<String>	Read-write	Type of security used for communications between the Citrix ADC and the LDAP server. For the PLAINTEXT setting, no encryption is required. Default value: TLS Possible values = PLAINTEXT, TLS, SSL
svrtype	<String>	Read-write	The type of LDAP server. Default value: AAA_LDAP_SERVER_TYPE_DEFAULT Possible values = AD, NDS
ssonameattribute	<String>	Read-write	Attribute used by the Citrix ADC to query an external LDAP server or Active Directory for an alternative username. This alternative username is then used for single sign-on (SSO).
passwdchange	<String>	Read-write	Accept password change requests.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: DISABLED Possible values = ENABLED, DISABLED
nestedgroupextraction	<String>	Read-write	Queries the external LDAP server to determine whether the specified group belongs to another group. Default value: OFF Possible values = ON, OFF
maxnestinglevel	<Integer>	Read-write	Number of levels up to which the system can query nested LDAP groups. Default value: 2 Minimum value = 2
groupnameidentifier	<String>	Read-write	LDAP-group attribute that uniquely identifies the group. No two groups on one LDAP server can have the same group name identifier.
groupsearchattribute	<String>	Read-write	LDAP-group attribute that designates the parent group of the specified group. Use this attribute to

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			search for a group's parent group.
groupsearchsubattribute	<String>	Read-write	LDAP-group subattribute that designates the parent group of the specified group. Use this attribute to search for a group's parent group.
groupsearchfilter	<String>	Read-write	Search-expression that can be specified for sending group-search requests to the LDAP server.
defaultauthenticationgroup	<String>	Read-write	This is the default group that is chosen when the authentication succeeds in addition to extracted groups. Maximum length = 64
groupauthname	<String>	Read-only	To associate AAA users with an AAA group, use the command "bind AAA group ... -username ...". You can bind different policies to each AAA group. Use the command

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			"bind AAA group ... -policy ...".
builtin	<String[]>	Read-only	Indicates that a variable is a built-in (SYSTEM INTERNAL) type. Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL
feature	<String>	Read-only	The feature to be checked while applying this config.
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- UPDATE
- UNSET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.
- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of

creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaaldapparams **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"aaaldapparams":{

"serverip":<String_value>,

"serverport":<Integer_value>,

"authtimeout":<Integer_value>,

"ldapbase":<String_value>,

"ldapbinddn":<String_value>,

"ldapbinddnpassword":<String_value>,

"ldaploginname":<String_value>,

"searchfilter":<String_value>,
```

```
"groupattrname":<String_value>,

"subattributename":<String_value>,

"sectype":<String_value>,

"svrtype":<String_value>,

"ssonameattribute":<String_value>,

"passwdchange":<String_value>,

"nestedgroupextraction":<String_value>,

"maxnestinglevel":<Integer_value>,

"groupnameidentifier":<String_value>,

"groupsearchattribute":<String_value>,

"groupsearchsubattribute":<String_value>,

"groupsearchfilter":<String_value>,

"defaultauthenticationgroup":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaaldapparams? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"aaaldapparams":{

"serverip":true,

"serverport":true,

"authtimeout":true,

"ldapbase":true,

"ldapbinddn":true,

"ldapbinddnpassword":true,

"ldaploginname":true,

"searchfilter":true,

"groupattrname":true,

"subattributename":true,

"sectype":true,

"svrtype":true,

"ssonameattribute":true,

"passwdchange":true,

"nestedgroupextraction":true,

"maxnestinglevel":true,

"groupnameidentifier":true,

"groupsearchattribute":true,

"groupsearchsubattribute":true,

"groupsearchfilter":true,
```

```
"defaultauthenticationgroup":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaaldapparams **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "aaaldapparams": [ {

"serverip":<String_value>,

"serverport":<Integer_value>,

"authtimeout":<Integer_value>,

"ldapbinddn":<String_value>,

"ldaploginname":<String_value>,

"ldapbase":<String_value>,
```

```
"sectype":<String_value>,

"svrtype":<String_value>,

"ssonameattribute":<String_value>,

"searchfilter":<String_value>,

"groupattrname":<String_value>,

"subattributename":<String_value>,

"groupauthname":<String_value>,

"passwdchange":<String_value>,

"nestedgroupextraction":<String_value>,

"maxnestinglevel":<Integer_value>,

"groupnameidentifier":<String_value>,

"groupsearchattribute":<String_value>,

"groupsearchsubattribute":<String_value>,

"groupsearchfilter":<String_value>,

"defaultauthenticationgroup":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

aaaotpparameter

Configuration for AAA otpparameter resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
encryption	<String>	Read-write	To encrypt otp secret in AD or not. Default value is OFF. Default value: OFF Possible values = ON, OFF
maxotpdevices	<Integer>	Read-write	Maximum number of otp devices user can register. Default value is 4. Max value is 255. Default value: 4 Minimum value = 0 Maximum value = 255
otptype	<String>	Read-write	Input flag to generate OTP for the given type. Possible values = gwtest
_nextgenapiresource	<String>	Read-only	.
gwtestchallenge	<String>	Read-only	Holds the generated OTP to access gwtest admin flow.

Operations

(click to see Properties)

- UPDATE
- UNSET

- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaaotpparameter **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"aaaotpparameter":{

"encryption":<String_value>,
```

```
"maxotpdevices":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaaotpparameter? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"aaaotpparameter":{

"encryption":true,

"maxotpdevices":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaaotpparameter **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "aaaotpparameter": [ {

"encryption":<String_value>,

"maxotpdevices":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

aaaparameter

Configuration for AAA parameter resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
enablestaticpagecaching	<String>	Read-write	The default state of VPN Static Page caching. Static Page caching is enabled by default. Default value: YES Possible values = YES, NO

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
enableenhancedauthfeedback	<String>	Read-write	Enhanced auth feedback provides more information to the end user about the reason for an authentication failure. The default value is set to NO. Default value: NO Possible values = YES, NO
defaultauthtype	<String>	Read-write	The default authentication server type. Default value: LOCAL Possible values = LOCAL, LDAP, RADIUS, TACACS, CERT
maxaaausers	<Integer>	Read-write	Maximum number of concurrent users allowed to log on to VPN simultaneously. Minimum value = 1
maxloginattempts	<Integer>	Read-write	Maximum Number of login Attempts. Minimum value = 1
failedlogintimeout	<Integer>	Read-write	Number of minutes an account will be locked if user exceeds maximum permissible attempts.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum value = 1 Maximum value = 525600
aaadnatip	<String>	Read-write	Source IP address to use for traffic that is sent to the authentication server.
enablesessionstickiness	<String>	Read-write	Enables/Disables stickiness to authentication servers. Default value: NO Possible values = YES, NO
aaasessionloglevel	<String>	Read-write	Audit log level, which specifies the types of events to log for cli executed commands. Available values function as follows: * EMERGENCY - Events that indicate an immediate crisis on the server. * ALERT - Events that might require action. * CRITICAL - Events that indicate

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			an imminent server crisis. * ERROR - Events that indicate some type of error. * WARNING - Events that require action in the near future. * NOTICE - Events that the administrator should know about. * INFORMATIONAL - All but low-level events. * DEBUG - All events, in extreme detail. Default value: DEFAULT_LOGLEVEL_AAA Possible values = EMERGENCY, ALERT, CRITICAL, ERROR, WARNING, NOTICE, INFORMATIONAL, DEBUG

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
aaadloglevel	<String>	Read-write	AAAD log level, which specifies the types of AAAD events to log in nsvpn.log. Available values function as follows: * EMERGENCY - Events that indicate an immediate crisis on the server. * ALERT - Events that might require action. * CRITICAL - Events that indicate an imminent server crisis. * ERROR - Events that indicate some type of error. * WARNING - Events that require action in the near future. * NOTICE - Events that the administrator should know about.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			* INFORMATIONAL - All but low-level events. * DEBUG - All events, in extreme detail. Default value: INFORMATIONAL Possible values = EMERGENCY, ALERT, CRITICAL, ERROR, WARNING, NOTICE, INFORMATIONAL, DEBUG
dynaddr	<String>	Read-write	Set by the DHCP client when the IP address was fetched dynamically. Default value: OFF Possible values = ON, OFF
ftmode	<String>	Read-write	First time user mode determines which configuration options are shown by default when logging in to the GUI. This setting is controlled by the GUI. Default value: ON

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ON, HA, OFF
maxsamldeflatesize	<Integer>	Read-write	This will set the maximum deflate size in case of SAML Redirect binding.
persistentloginattempts	<String>	Read-write	Persistent storage of unsuccessful user login attempts. Default value: DISABLED Possible values = ENABLED, DISABLED
pwdexpirynotificationdays	<Integer>	Read-write	This will set the threshold time in days for password expiry notification. Default value is 0, which means no notification is sent.
maxkbquestions	<Integer>	Read-write	This will set maximum number of Questions to be asked for KB Validation. Default value is 2, Max Value is 6. Minimum value = 2 Maximum value = 6
loginencryption	<String>	Read-write	Parameter to encrypt login information for nFactor flow.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: DISABLED Possible values = ENABLED, DISABLED
samesite	<String>	Read-write	SameSite attribute value for Cookies generated in AAATM context. This attribute value will be appended only for the cookies which are specified in the builtin patset ns_cookies_samesite. Possible values = None, LAX, STRICT
apitokencache	<String>	Read-write	Option to enable/disable API cache feature. Default value: DISABLED Possible values = ENABLED, DISABLED
tokenintrospectioninterval	<Integer>	Read-write	Frequency at which a token must be verified at the Authorization Server (AS) despite being found in cache.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
defaultcspheader	<String>	Read-write	Parameter to enable/disable default CSP header. Default value: ENABLED Possible values = ENABLED, DISABLED
classicendpoints	<String>	Read-write	Parameter to enable/disable classic endpoints. Default value: ENABLED Possible values = ENABLED, DISABLED
webviewendpoints	<String>	Read-write	Parameter to enable/disable webview endpoints. Default value: ENABLED Possible values = ENABLED, DISABLED
httponlycookie	<String>	Read-write	Parameter to set/reset HttpOnly Flag for NSC_AAAC/NSC_TMAS cookies in nfactor. Default value: ENABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ENABLED, DISABLED
enhancedepa	<String>	Read-write	Parameter to enable/disable EPA v2 functionality. Default value: DISABLED Possible values = ENABLED, DISABLED
wafprotection	<String[]>	Read-write	Entities for which WAF Protection need to be applied. Available settings function as follows: * DEFAULT - AUTH, VPN and PORTAL Protections are enabled. This is the default value for wafProtection * AUTH - Endpoints used for Authentication applicable for both AAATM, IDP, GATEWAY use cases. * VPN - Endpoints used for Gateway use cases.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			* PORTAL - Endpoints related to web portal. * DISABLED - No Endpoint WAF protection. Currently supported only in default partition. Default value: DEFAULT Possible values = DISABLED, AUTH, VPN, PORTAL, DEFAULT
securityinsights	<String>	Read-write	On enabling this option, the Citrix ADC will send the security insight records to the configured collectors when request comes to Authentication endpoint. * If cs vserver is frontend with Authentication vserver as target for cs action, then record is sent using Authentication vserver name.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			* If vpn/lb/cs vserver are configured with Authentication ON, then then record is sent using vpn/lb/cs vserver name accordingly. * If authentication vserver is frontend, then record is sent using Authentication vserver name. Default value: DISABLED Possible values = ENABLED, DISABLED
builtin	<String[]>	Read-only	Flag to determine if aaa param is built-in or not. Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL
feature	<String>	Read-only	The feature to be checked while applying this config.
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- UPDATE
- UNSET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaaparameter **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"aaaparameter":{

"enablestaticpagecaching":<String_value>,

"enableenhancedauthfeedback":<String_value>,

"defaultauthtype":<String_value>,

"maxaaausers":<Integer_value>,

"maxloginattempts":<Integer_value>,

"failedlogintimeout":<Integer_value>,

"aaadnatip":<String_value>,

"enablesessionstickiness":<String_value>,

"aaasessionloglevel":<String_value>,

"aaadloglevel":<String_value>,

"dynaddr":<String_value>,

"ftmode":<String_value>,

"maxsamldeflatesize":<Integer_value>,

"persistentloginattempts":<String_value>,

"pwdexpirynotificationdays":<Integer_value>,

"maxkbquestions":<Integer_value>,

"loginencryption":<String_value>,

"samesite":<String_value>,

"apitokencache":<String_value>,

"tokenintrospectioninterval":<Integer_value>,

"defaultcspheader":<String_value>,
```

```
"classicendpoints":<String_value>,

"webviewendpoints":<String_value>,

"httponlycookie":<String_value>,

"enhancedepa":<String_value>,

"wafprotection":<String[]_value>,

"securityinsights":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaaparameter? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"aaaparameter":{

"enablestaticpagecaching":true,

"enableenhancedauthfeedback":true,

"defaultauthtype":true,

"maxaaausers":true,
```

```
"aaadnatip":true,

"maxloginattempts":true,

"enablesessionstickiness":true,

"maxsamldeflatesize":true,

"persistentloginattempts":true,

"pwdexpirynotificationdays":true,

"maxkbquestions":true,

"aaasessionloglevel":true,

"aaadloglevel":true,

"dynaddr":true,

"ftmode":true,

"loginencryption":true,

"samesite":true,

"apitokencache":true,

"tokenintrospectioninterval":true,

"defaultcspheader":true,

"classicendpoints":true,

"webviewendpoints":true,

"httponlycookie":true,

"enhancedepa":true,

"wafprotection":true,

"securityinsights":true
```

```
}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaaparameter **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "aaaparameter": [ {

"enablestaticpagecaching":<String_value>,

"enableenhancedauthfeedback":<String_value>,

"defaultauthtype":<String_value>,

"maxaaausers":<Integer_value>,

"aaadnatip":<String_value>,

"maxloginattempts":<Integer_value>,

"failedlogintimeout":<Integer_value>,
```

```
"enablesessionstickiness":<String_value>,

"aaasessionloglevel":<String_value>,

"aaadloglevel":<String_value>,

"dynaddr":<String_value>,

"ftmode":<String_value>,

"maxsamldeflatesize":<Integer_value>,

"persistentloginattempts":<String_value>,

"pwdexpirynotificationdays":<Integer_value>,

"maxkbquestions":<Integer_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"loginencryption":<String_value>,

"samesite":<String_value>,

"apitokencache":<String_value>,

"tokenintrospectioninterval":<Integer_value>,

"defaultcspheader":<String_value>,

"classicendpoints":<String_value>,

"webviewendpoints":<String_value>,

"httponlycookie":<String_value>,

"enhancedepa":<String_value>,

"wafprotection":<String[]_value>,

"securityinsights":<String_value>,
```

```
"_nextgenapiresource":<String_value>

}]}
```

aaapreauthenticationaction

Configuration for pre authentication action resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the preauthentication action. Must begin with a letter, number, or the underscore character (_), and must consist only of letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after preauthentication action is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			marks (for example, "my aaa action" or 'my aaa action'). Minimum length = 1
preauthenticationaction	<String>	Read-write	Allow or deny logon after endpoint analysis (EPA) results. Possible values = ALLOW, DENY
killprocess	<String>	Read-write	String specifying the name of a process to be terminated by the endpoint analysis (EPA) tool.
deletefiles	<String>	Read-write	String specifying the path(s) and name(s) of the files to be deleted by the endpoint analysis (EPA) tool.
defaultepagroup	<String>	Read-write	This is the default group that is chosen when the EPA check succeeds. Maximum length = 64
builtin	<String[]>	Read-only	Indicates that a variable is a built-in (SYSTEM INTERNAL) type. Possible values = MODIFIABLE, DELETABLE,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			IMMUTABLE, PARTITION_ALL
feature	<String>	Read-only	The feature to be checked while applying this config.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaapreauthenticationaction **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"aaapreauthenticationaction":{

<b>"name":<String_value>,

</b>"preauthenticationaction":<String_value>,

"killprocess":<String_value>,

"deletefiles":<String_value>,

"defaultepagroup":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaapreauthenticationaction/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaapreauthenticationaction **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"aaapreauthenticationaction":{

<b>"name":<String_value>,

</b>"preauthenticationaction":<String_value>,

"killprocess":<String_value>,

"deletefiles":<String_value>,

"defaultepagroup":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaapreauthenticationaction? **action=unset**
HTTP Method: POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"aaapreauthenticationaction":{

<b>"name":<String_value>,

</b>"killprocess":true,

"deletefiles":true,

"defaultepagroup":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaapreauthenticationaction **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/aaapreauthenticationaction? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/aaapreauthenticationaction? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of aaapreauthenticationaction resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/aaapreauthenticationaction? **view=summary**

Use this query-parameter to get the summary output of aaapreauthenticationaction resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/aaapreauthenticationaction? **pagesize=#no;pageno=#no**

Use this query-parameter to get the aaapreauthenticationaction resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "aaapreauthenticationaction": [ {

"name":<String_value>,

"preauthenticationaction":<String_value>,

"killprocess":<String_value>,

"deletefiles":<String_value>,

"builtin":<String[]_value>,
```

```
"feature":<String_value>,

"defaultepagroup":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaapreauthenticationaction/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/ aaapreauthenticationaction/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/aaapreauthenticationaction/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of aaapreauthenticationaction resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "aaapreauthenticationaction": [ {

"name":<String_value>,

"preauthenticationaction":<String_value>,

"killprocess":<String_value>,

"deletefiles":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"defaultepagroup":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaapreauthenticationaction? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "aaapreauthenticationaction": [ { "__count": "#no"} ] }
```

aaapreauthenticationparameter

Configuration for pre authentication parameter resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
preauthenticationaction	<String>	Read-write	Deny or allow login on the basis of end point analysis results. Possible values = ALLOW, DENY
rule	<String>	Read-write	Name of the Citrix ADC named rule, or an expression, to be evaluated by the EPA tool.
killprocess	<String>	Read-write	String specifying the name of a process to be terminated by the EPA tool.
deletefiles	<String>	Read-write	String specifying the path(s) to and name(s) of the files to be deleted by the EPA tool, as a string of between 1 and 1023 characters.
builtin	<String[]>	Read-only	Indicates that a variable is a built-in (SYSTEM INTERNAL) type.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL
feature	<String>	Read-only	The feature to be checked while applying this config.
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- UPDATE
- UNSET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaapreauthenticationparameter **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"aaapreauthenticationparameter":{

"preauthenticationaction":<String_value>,

"rule":<String_value>,

"killprocess":<String_value>,

"deletefiles":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaapreauthenticationparameter? **action=unset** **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"aaapreauthenticationparameter":{

"rule":true,

"preauthenticationaction":true,

"killprocess":true,

"deletefiles":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaapreauthenticationparameter **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "aaapreauthenticationparameter": [ {

"preauthenticationaction":<String_value>,

"rule":<String_value>,

"killprocess":<String_value>,

"deletefiles":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

aaapreauthenticationpolicy

Configuration for pre authentication policy resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the preauthentication policy. Must begin with a letter, number, or the underscore character (_), and must consist only of letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			characters. Cannot be changed after the preauthentication policy is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my policy" or 'my policy'). Minimum length = 1
rule	<String>	Read-write	Name of the Citrix ADC named rule, or an expression, defining connections that match the policy.
reqaction	<String>	Read-write	Name of the action that the policy is to invoke when a connection matches the policy. Minimum length = 1
hits	<Integer>	Read-only	No of hits.
builtin	<String[]>	Read-only	Indicates that a variable is a built-in (SYSTEM INTERNAL) type.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL
feature	<String>	Read-only	The feature to be checked while applying this config.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of

creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaapreauthenticationpolicy **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"aaapreauthenticationpolicy":{

<b>"name":<String_value>,

</b><b>"rule":<String_value>,

</b>"reqaction":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaapreauthenticationpolicy/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaapreauthenticationpolicy **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"aaapreauthenticationpolicy":{

<b>"name":<String_value>,

</b>"rule":<String_value>,

"reqaction":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaapreauthenticationpolicy **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/aaapreauthenticationpolicy? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/aaapreauthenticationpolicy? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of aaapreauthenticationpolicy resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/aaapreauthenticationpolicy? **view=summary**

Use this query-parameter to get the summary output of aaapreauthenticationpolicy resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/aaapreauthenticationpolicy? **pagesize=#no;pageno=#no**

Use this query-parameter to get the aaapreauthenticationpolicy resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "aaapreauthenticationpolicy": [ {

"name":<String_value>,

"rule":<String_value>,

"reqaction":<String_value>,

"hits":<Integer_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaapreauthenticationpolicy/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/ aaapreauthenticationpolicy/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/aaapreauthenticationpolicy/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of aaapreauthenticationpolicy resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "aaapreauthenticationpolicy": [ {

"name":<String_value>,

"rule":<String_value>,

"reqaction":<String_value>,

"hits":<Integer_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaapreauthenticationpolicy? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "aaapreauthenticationpolicy": [ { "__count": "#no"} ] }
```

aaapreauthenticationpolicy_aaaglobal_binding

Binding object showing the aaaglobal that can be bound to aaapreauthenticationpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
boundto	<String>	Read-write	The entity name to which policy is bound.
name	<String>	Read-write	Name of the preauthentication policy whose properties you want to view. Minimum length = 1
activepolicy	<Integer>	Read-only	.
priority	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaapreauthenticationpolicy_aaaglobal_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ aaapreauthenticationpolicy_aaaglobal_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of aaapreauthenticationpolicy_aaaglobal_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ aaapreauthenticationpolicy_aaaglobal_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the aaapreauthenticationpolicy_aaaglobal_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "aaapreauthenticationpolicy_aaaglobal_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"activepolicy":<Integer_value>,

"priority":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaapreauthenticationpolicy_aaaglobal_binding
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/aaapreauthenticationpolicy_aaaglobal_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "aaapreauthenticationpolicy_aaaglobal_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"activepolicy":<Integer_value>,

"priority":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaapreauthenticationpolicy_aaaglobal_binding/name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"aaapreauthenticationpolicy_aaaglobal_binding": [ { "__count": "#no"} ] }
```

aaapreauthenticationpolicy_binding

Binding object which returns the resources bound to aaapreauthenticationpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the preauthentication policy whose properties you want to view. Minimum length = 1
aaapreauthenticationpolicy_aaaglobal_binding	<aaapreauthenticationpolicy_aaaglobal_binding[]>	Read-only	aaaglobal that can be bound to aaapreauthentication policy.
aaapreauthenticationpolicy_vpnvserver_binding	<aaapreauthenticationpolicy_vpnvserver_binding[]>	Read-only	vpnvserver that can be bound to aaapreauthentication policy.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaapreauthenticationpolicy_binding/name_value<String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "aaapreauthenticationpolicy_binding": [ {

"name":<String_value>,

"aaapreauthenticationpolicy_vpnvserver_binding":<aaapreauthenticationpolic
y_vpnvserver_binding[]_value>,

"aaapreauthenticationpolicy_aaaglobal_binding":<aaapreauthenticationpolicy
_aaaglobal_binding[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaapreauthenticationpolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/aaapreauthenticationpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "aaapreauthenticationpolicy_binding": [ {

"name":<String_value>,

"aaapreauthenticationpolicy_vpnvserver_binding":<aaapreauthenticationpolic
y_vpnvserver_binding[]_value>,

"aaapreauthenticationpolicy_aaaglobal_binding":<aaapreauthenticationpolicy
_aaaglobal_binding[]_value>

}]}
```

aaapreauthenticationpolicy_vpnvserver_binding

Binding object showing the vpnvserver that can be bound to aaapreauthenticationpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
boundto	<String>	Read-write	The entity name to which policy is bound.
name	<String>	Read-write	Name of the preauthentication policy whose properties you want to view. Minimum length = 1
priority	<Integer>	Read-only	.
activepolicy	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaapreauthenticationpolicy_vpnvserver_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/aaapreauthenticationpolicy_vpnvserver_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of aaapreauthenticationpolicy_vpnvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ aaapreauthenticationpolicy_vpnvserver_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the aaapreauthenticationpolicy_vpnvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "aaapreauthenticationpolicy_vpnvserver_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"priority":<Integer_value>,

"activepolicy":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/ aaapreauthenticationpolicy_vpnvserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ aaapreauthenticationpolicy_vpnvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "aaapreauthenticationpolicy_vpnvserver_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"priority":<Integer_value>,

"activepolicy":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/ aaapreauthenticationpolicy_vpnvserver_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"aaapreauthenticationpolicy_vpnvserver_binding": [ { "__count":
"#no"} ] }
```

aaaproxyparam

Configuration for AAA proxy parameter resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
proxy	<String>	Read-write	IP address and Port of the proxy server to be used for HTTP access for this request. This can be configured in the following manner: First way is to configure in ipaddress:port format like a.b.c.d:e or this can be specified via the alternate format which is to specify like http://a.b.c.d

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			without port or http://a.b.c.d:8080 with port. Minimum length = 1
proxyauthorization	<String>	Read-write	this indicates whether Proxy-Authorization header will be sent or not. Default value: PROXY_AUTH_DISABLED Possible values = disabled, basic
proxyusername	<String>	Read-write	username that will be sent as part of Basic Proxy-Authorization header. Maximum length = 256
proxypassword	<String>	Read-write	password that will be sent as part of Basic Proxy-Authorization header. Maximum length = 256
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- UPDATE
- UNSET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaaproxyparam **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"aaaproxyparam":{

"proxy":<String_value>,

"proxyauthorization":<String_value>,
```

```
"proxyusername":<String_value>,

"proxypassword":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaaproxyparam? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"aaaproxyparam":{

"proxy":true,

"proxyauthorization":true,

"proxyusername":true,

"proxypassword":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaaproxyparam **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "aaaproxyparam": [ {

"proxy":<String_value>,

"proxyauthorization":<String_value>,

"proxyusername":<String_value>,

"proxypassword":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

aaaradiusparams

Configuration for RADIUS parameter resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
serverip	<String>	Read-write	IP address of your RADIUS server. Minimum length = 1
serverport	<Integer>	Read-write	Port number on which the RADIUS server listens for connections. Default value: 1812 Minimum value = 1
authtimeout	<Integer>	Read-write	Maximum number of seconds that the Citrix ADC waits for a response from the RADIUS server. Default value: 3 Minimum value = 1
radkey	<String>	Read-write	The key shared between the RADIUS server and clients. Required for allowing the Citrix ADC to communicate with the RADIUS server. Minimum length = 1
radnasip	<String>	Read-write	Send the Citrix ADC IP (NSIP) address to the RADIUS server as the Network Access Server IP (NASIP) part of the Radius protocol.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ENABLED, DISABLED
radnasid	<String>	Read-write	Send the Network Access Server ID (NASID) for your Citrix ADC to the RADIUS server as the nasid part of the Radius protocol.
radvendorid	<Integer>	Read-write	Vendor ID for RADIUS group extraction. Minimum value = 1
radattributetype	<Integer>	Read-write	Attribute type for RADIUS group extraction. Minimum value = 1
radgroupsprefix	<String>	Read-write	Prefix string that precedes group names within a RADIUS attribute for RADIUS group extraction.
radgroupseparator	<String>	Read-write	Group separator string that delimits group names within a RADIUS attribute for RADIUS group extraction.
passencoding	<String>	Read-write	Enable password encoding in RADIUS packets that the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Citrix ADC sends to the RADIUS server. Default value: mschapv2 Possible values = pap, chap, mschapv1, mschapv2
ipvendorid	<Integer>	Read-write	Vendor ID attribute in the RADIUS response. If the attribute is not vendor-encoded, it is set to 0.
ipattributetype	<Integer>	Read-write	IP attribute type in the RADIUS response. Minimum value = 1
accounting	<String>	Read-write	Configure the RADIUS server state to accept or refuse accounting messages. Possible values = ON, OFF
pwdvendorid	<Integer>	Read-write	Vendor ID of the password in the RADIUS response. Used to extract the user password. Minimum value = 1
pwdattributetype	<Integer>	Read-write	Attribute type of the Vendor ID in the RADIUS response.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum value = 1
defaultauthentication group	<String>	Read-write	This is the default group that is chosen when the authentication succeeds in addition to extracted groups. Maximum length = 64
callingstationid	<String>	Read-write	Send Calling-Station-ID of the client to the RADIUS server. IP Address of the client is sent as its Calling-Station-ID. Default value: DISABLED Possible values = ENABLED, DISABLED
authservretry	<Integer>	Read-write	Number of retry by the Citrix ADC before getting response from the RADIUS server. Default value: 3 Minimum value = 1 Maximum value = 10
authentication	<String>	Read-write	Configure the RADIUS server state to accept or refuse

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			authentication messages. Default value: ON Possible values = ON, OFF
tunnelendpointclientip	<String>	Read-write	Send Tunnel Endpoint Client IP address to the RADIUS server. Default value: DISABLED Possible values = ENABLED, DISABLED
messageauthenticator	<String>	Read-write	Control whether the Message-Authenticator attribute is included in a RADIUS Access-Request packet. Default value: ON Possible values = ON, OFF
groupauthname	<String>	Read-only	To associate AAA users with an AAA group, use the command "bind AAA group ... -username ...". You can bind different policies to

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			each AAA group. Use the command "bind AAA group ... -policy ...".
ipaddress	<String>	Read-only	IP Address.
builtin	<String[]>	Read-only	Indicates that a variable is a built-in (SYSTEM INTERNAL) type. Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL
feature	<String>	Read-only	The feature to be checked while applying this config.
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- UPDATE
- UNSET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaaradiusparams **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"aaaradiusparams":{

"serverip":<String_value>,

"serverport":<Integer_value>,

"authtimeout":<Integer_value>,

<b>"radkey":<String_value>,

</b>"radnasip":<String_value>,

"radnasid":<String_value>,
```

```
"radvendorid":<Integer_value>,

"radattributetype":<Integer_value>,

"radgroupsprefix":<String_value>,

"radgroupseparator":<String_value>,

"passencoding":<String_value>,

"ipvendorid":<Integer_value>,

"ipattributetype":<Integer_value>,

"accounting":<String_value>,

"pwdvendorid":<Integer_value>,

"pwdattributetype":<Integer_value>,

"defaultauthenticationgroup":<String_value>,

"callingstationid":<String_value>,

"authservretry":<Integer_value>,

"authentication":<String_value>,

"tunnelendpointclientip":<String_value>,

"messageauthenticator":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaaradiusparams? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"aaaradiusparams":{

"serverip":true,

"serverport":true,

"authtimeout":true,

"radnasip":true,

"radnasid":true,

"radvendorid":true,

"radattributetype":true,

"radgroupsprefix":true,

"radgroupseparator":true,

"passencoding":true,

"ipvendorid":true,

"ipattributetype":true,

"accounting":true,

"pwdvendorid":true,

"pwdattributetype":true,
```

```
"defaultauthenticationgroup":true,

"callingstationid":true,

"authservretry":true,

"authentication":true,

"tunnelendpointclientip":true,

"messageauthenticator":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaaradiusparams **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "aaaradiusparams": [ {

"serverip":<String_value>,
```

```
"serverport":<Integer_value>,

"radkey":<String_value>,

"groupauthname":<String_value>,

"authtimeout":<Integer_value>,

"radnasip":<String_value>,

"radnasid":<String_value>,

"ipaddress":<String_value>,

"radvendorid":<Integer_value>,

"radattributetype":<Integer_value>,

"radgroupsprefix":<String_value>,

"radgroupseparator":<String_value>,

"passencoding":<String_value>,

"ipvendorid":<Integer_value>,

"ipattributetype":<Integer_value>,

"accounting":<String_value>,

"pwdvendorid":<Integer_value>,

"pwdattributetype":<Integer_value>,

"defaultauthenticationgroup":<String_value>,

"callingstationid":<String_value>,

"authservretry":<Integer_value>,

"authentication":<String_value>,

"tunnelendpointclientip":<String_value>,
```

```
"builtin":<String[]_value>,

"feature":<String_value>,

"messageauthenticator":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

aaasession

Configuration for active connection resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
username	<String>	Read-write	Name of the AAA user. Minimum length = 1
groupname	<String>	Read-write	Name of the AAA group. Minimum length = 1
iip	<String>	Read-write	IP address or the first address in the intranet IP range. Minimum length = 1
netmask	<String>	Read-write	Subnet mask for the intranet IP range. Minimum length = 1
sessionkey	<String>	Read-write	Show aaa session associated with given session key.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum length = 1 Maximum length = 127
nodeid	<Integer>	Read-write	Unique number that identifies the cluster node. Minimum value = 0 Maximum value = 31
all	<Boolean>	Read-write	Terminate all active AAA-TM/VPN sessions.
publicip	<String>	Read-only	Client's public IP address.
publicport	<Integer>	Read-only	Client's public port. Range 1 - 65535 * in CLI is represented as 65535 in NITRO API
ipaddress	<String>	Read-only	Citrix ADC's IP address.
port	<Integer>	Read-only	Citrix ADC's port. Range 1 - 65535 * in CLI is represented as 65535 in NITRO API

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
privateip	<String>	Read-only	Client's private/ mapped IP address.
privateport	<Integer>	Read-only	Client's private/ mapped port. Range 1 - 65535 * in CLI is represented as 65535 in NITRO API
destip	<String>	Read-only	Destination IP address.
destport	<Integer>	Read-only	Destination port. Range 1 - 65535 * in CLI is represented as 65535 in NITRO API
intranetip	<String>	Read-only	Specifies the Intranet IP.
intranetip6	<String>	Read-only	Specifies the Intranet IP6.
peid	<Integer>	Read-only	Core id of the session owner.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET (ALL)

- COUNT
- KILL

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

KILL

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaasession? **action=kill HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"aaasession":{

"username":<String_value>,

"groupname":<String_value>,

"iip":<String_value>,

"netmask":<String_value>,

"sessionkey":<String_value>,

"all":<Boolean_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaasession **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/aaasession? **args=username: <String_value> ,groupname: <String_value> ,iip: <String_value> ,netmask: <String_value> ,sessionkey: <String_value> ,nodeid: <Integer_value>**

Use this query-parameter to get aaasession resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/config/aaasession? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/aaasession? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of aaasession resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/aaasession? **view=summary**

Use this query-parameter to get the summary output of aaasession resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/aaasession? **pagesize=#no;pageno=#no**

Use this query-parameter to get the aaasession resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "aaasession": [ {

username:<String_value>,groupname:<String_value>,iip:<String_value>,netmas
k:<String_value>,sessionkey:<String_value>,nodeid:<Integer_value>"publicip
":<String_value>,

"publicport":<Integer_value>,

"ipaddress":<String_value>,

"port":<Integer_value>,

"privateip":<String_value>,

"privateport":<Integer_value>,
```

```
"destip":<String_value>,

"destport":<Integer_value>,

"intranetip":<String_value>,

"intranetip6":<String_value>,

"peid":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaasession? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "aaasession": [ { "__count": "#no"} ] }
```

aaassoprofile

Configuration for aaa sso profile resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the SSO Profile. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after a SSO Profile is created. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my action" or 'my action'). Minimum length = 1
username	<String>	Read-write	Name for the user. Must begin with a letter, number, or the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			underscore (_) character, and must contain only alphanumeric, hyphen (-), period (.), hash (#), space ( ), at (@), equal (=), colon (:), and underscore characters. CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my group" or 'my group'). Minimum length = 1
password	<String>	Read-write	Password with which the user logs on. Required for Single sign on to external server. Minimum length = 1
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET (ALL)

- GET
- COUNT
- UPDATE

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaassoprofile **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"aaassoprofile":{

<b>"name":<String_value>,

</b><b>"username":<String_value>,

</b><b>"password":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaassoprofile/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaassoprofile **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"aaassoprofile":{

<b>"name":<String_value>,
```

```
</b>"username":<String_value>,

"password":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaassoprofile **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/aaassoprofile? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/aaassoprofile? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of aaassoprofile resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/aaassoprofile? **view=summary**

Use this query-parameter to get the summary output of aaassoprofile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/aaassoprofile? **pagesize=#no;pageno=#no**

Use this query-parameter to get the aaassoprofile resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "aaassoprofile": [ {

"name":<String_value>,

"username":<String_value>,

"password":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaassoprofile/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/aaassoprofile/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/aaassoprofile/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of aaassoprofile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "aaassoprofile": [ {

"name":<String_value>,

"username":<String_value>,

"password":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaassoprofile? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "aaassoprofile": [ { "__count": "#no"} ] }
```

aaatacacsparams

Configuration for tacacs parameters resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
serverip	<String>	Read-write	IP address of your TACACS+ server. Minimum length = 1
serverport	<Integer>	Read-write	Port number on which the TACACS+ server listens for connections. Default value: 49 Minimum value = 1
authtimeout	<Integer>	Read-write	Maximum number of seconds that the Citrix ADC waits for a response from the TACACS+ server. Default value: 3 Minimum value = 1
tacacssecret	<String>	Read-write	Key shared between the TACACS+ server and clients. Required for allowing the Citrix ADC to communicate

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			with the TACACS+ server. Minimum length = 1
authorization	<String>	Read-write	Use streaming authorization on the TACACS+ server. Possible values = ON, OFF
accounting	<String>	Read-write	Send accounting messages to the TACACS+ server. Possible values = ON, OFF
auditfailedcmds	<String>	Read-write	The option for sending accounting messages to the TACACS+ server. Possible values = ON, OFF
groupattrname	<String>	Read-write	TACACS+ group attribute name.Used for group extraction on the TACACS+ server.
defaultauthentication group	<String>	Read-write	This is the default group that is chosen when the authentication succeeds in addition to extracted groups. Maximum length = 64
builtin	<String[]>	Read-only	Indicates that a variable is a built-in

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			(SYSTEM INTERNAL) type. Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL
feature	<String>	Read-only	The feature to be checked while applying this config.
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- UPDATE
- UNSET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaatacacsparams? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"aaatacacsparams":{

"serverip":true,

"serverport":true,

"authtimeout":true,

"tacacssecret":true,

"authorization":true,

"accounting":true,

"auditfailedcmds":true,

"groupattrname":true,

"defaultauthenticationgroup":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaatacacsparams **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"aaatacacsparams":{

"serverip":<String_value>,

"serverport":<Integer_value>,

"authtimeout":<Integer_value>,

"tacacssecret":<String_value>,

"authorization":<String_value>,

"accounting":<String_value>,

"auditfailedcmds":<String_value>,

"groupattrname":<String_value>,

"defaultauthenticationgroup":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaatacacsparams **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "aaatacacsparams": [ {

"serverip":<String_value>,

"serverport":<Integer_value>,

"authtimeout":<Integer_value>,

"tacacssecret":<String_value>,

"authorization":<String_value>,

"accounting":<String_value>,

"auditfailedcmds":<String_value>,

"groupattrname":<String_value>,

"defaultauthenticationgroup":<String_value>,

"builtin":<String[]_value>,
```

```
"feature":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

aaauser

Configuration for AAA user resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
username	<String>	Read-write	Name for the user. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after the user is added. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			single quotation marks (for example, "my aaa user" or "my aaa user"). Minimum length = 1
password	<String>	Read-write	Password with which the user logs on. Required for any user account that does not exist on an external authentication server. If you are not using an external authentication server, all user accounts must have a password. If you are using an external authentication server, you must provide a password for local user accounts that do not exist on the authentication server. Minimum length = 1
loggedin	<Boolean>	Read-write	Show whether the user is logged in or not.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- GET (ALL)
- GET
- COUNT
- UNLOCK

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaauser **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"aaauser":{

<b>"username":<String_value>,

</b>"password":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNLOCK

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaauser? **action=unlock HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"aaauser":{

<b>"username":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaauser/ username_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaauser **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"aaauser":{

<b>"username":<String_value>,

</b><b>"password":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaauser **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/aaauser? **args=username: <String_value> ,loggedin: <Boolean_value>**

Use this query-parameter to get aaauser resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/config/aaauser? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/aaauser? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of aaauser resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/aaauser? **view=summary**

Use this query-parameter to get the summary output of aaauser resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/aaauser? **pagesize=#no;pageno=#no**

Use this query-parameter to get the aaauser resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "aaauser": [ {

username:<String_value>,loggedin:<Boolean_value>"password":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaauser/ username_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/aaauser/ username_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/aaauser/ username_value<String> ? **view=summary**

Use this query-parameter to get the summary output of aaauser resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "aaauser": [ {

username:<String_value>,loggedin:<Boolean_value>"password":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaauser? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "aaauser": [ { "__count": "#no"} ] }
```

aaauser_aaagroup_binding

Binding object showing the aaagroup that can be bound to aaauser.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
groupname	<String>	Read-write	The group name.
username	<String>	Read-write	User account to which to bind the policy. Minimum length = 1
gotopriorityexpression	<String>	Read-write	Expression or other value specifying the next policy to evaluate if the current policy evaluates to TRUE. Specify one of the following values: * NEXT - Evaluate the policy with the next higher priority number. * END - End policy evaluation. * USE_INVOCATION_RESULT - Applicable if this policy invokes another policy label. If the final goto in the invoked policy label has a value of END, the evaluation stops. If the final goto is anything other than END, the current policy label performs a NEXT. * An expression that

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			evaluates to a number. If you specify an expression, the number to which it evaluates determines the next policy to evaluate, as follows: * If the expression evaluates to a higher numbered priority, the policy with that priority is evaluated next. * If the expression evaluates to the priority of the current policy, the policy with the next higher numbered priority is evaluated next. * If the expression evaluates to a number that is larger than the largest numbered priority, policy evaluation ends. An UNDEF event is triggered if: * The expression is invalid. * The expression evaluates to a priority number that is numerically lower than the current policy's priority. * The expression evaluates to a priority number that is between the current policy's

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			priority number (say, 30) and the highest priority number (say, 100), but does not match any configured priority number (for example, the expression evaluates to the number 85). This example assumes that the priority number increments by 10 for every successive policy, and therefore a priority number of 85 does not exist in the policy label.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaauser_aaagroup_binding/ username_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ aaauser_aaagroup_binding/ username_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of aaauser_aaagroup_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/aaauser_aaagroup_binding/ username_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the aaauser_aaagroup_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "aaauser_aaagroup_binding": [ {

"groupname":<String_value>,

"username":<String_value>,

"gotopriorityexpression":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaauser_aaagroup_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/aaauser_aaagroup_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "aaauser_aaagroup_binding": [ {

"groupname":<String_value>,

"username":<String_value>,

"gotopriorityexpression":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaauser_aaagroup_binding/ username_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"aaauser_aaagroup_binding": [ { "__count": "#no"} ] }
```

aaauser_auditnslogpolicy_binding

Binding object showing the auditnslogpolicy that can be bound to aaauser.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
type	<String>	Read-write	Bindpoint to which the policy is bound. Default value: REQUEST Possible values = REQUEST, UDP_REQUEST, DNS_REQUEST, ICMP_REQUEST
priority	<Integer>	Read-write	Integer specifying the priority of the policy. A lower number indicates a higher priority. Policies are evaluated in the order of their priority numbers. Maximum value for default syntax policies is 2147483647 and for classic policies max priority is 64000. . Minimum value = 0 Maximum value = 2147483647
username	<String>	Read-write	User account to which to bind the policy. Minimum length = 1
gotopriorityexpression	<String>	Read-write	Expression or other value specifying the next policy to evaluate if the current policy

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			evaluates to TRUE. Specify one of the following values: * NEXT - Evaluate the policy with the next higher priority number. * END - End policy evaluation. * USE_INVOCATION_RESULT - Applicable if this policy invokes another policy label. If the final goto in the invoked policy label has a value of END, the evaluation stops. If the final goto is anything other than END, the current policy label performs a NEXT. * An expression that evaluates to a number. If you specify an expression, the number to which it evaluates determines the next policy to evaluate, as follows: * If the expression evaluates to a higher numbered priority, the policy with that priority is evaluated next. * If the expression evaluates to the priority of the current policy, the policy with the next

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			higher numbered priority is evaluated next. * If the expression evaluates to a number that is larger than the largest numbered priority, policy evaluation ends. An UNDEF event is triggered if: * The expression is invalid. * The expression evaluates to a priority number that is numerically lower than the current policy's priority. * The expression evaluates to a priority number that is between the current policy's priority number (say, 30) and the highest priority number (say, 100), but does not match any configured priority number (for example, the expression evaluates to the number 85). This example assumes that the priority number increments by 10 for every successive policy, and therefore a priority number of 85 does not exist in the policy label.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
policy	<String>	Read-write	The policy Name.
acttype	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/aaauser_auditnslogpolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"aaauser_auditnslogpolicy_binding":{

<b>"username":<String_value>,

</b>"policy":<String_value>,

"priority":<Integer_value>,

"type":<String_value>,

"gotopriorityexpression":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaauser_auditnslogpolicy_binding/ username_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/

aaauser_auditnslogpolicy_binding/ username_value<String> ? **args=policy: <String_value> ,type: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaauser_auditnslogpolicy_binding/ username_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ aaauser_auditnslogpolicy_binding/ username_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of aaauser_auditnslogpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/aaauser_auditnslogpolicy_binding/ username_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the aaauser_auditnslogpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "aaauser_auditnslogpolicy_binding": [ {

"type":<String_value>,

"priority":<Integer_value>,

"username":<String_value>,

"gotopriorityexpression":<String_value>,

"policy":<String_value>,

"acttype":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaauser_auditnslogpolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/aaauser_auditnslogpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "aaauser_auditnslogpolicy_binding": [ {

"type":<String_value>,

"priority":<Integer_value>,

"username":<String_value>,

"gotopriorityexpression":<String_value>,

"policy":<String_value>,

"acttype":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaauser_auditnslogpolicy_binding/ username_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"aaauser_auditnslogpolicy_binding": [ { "__count": "#no"} ] }
```

aaauser_auditsyslogpolicy_binding

Binding object showing the auditsyslogpolicy that can be bound to aaauser.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
gotopriorityexpression	<String>	Read-write	Expression or other value specifying the next policy to evaluate if the current policy evaluates to TRUE. Specify one of the following values: * NEXT - Evaluate the policy with the next higher priority number. * END - End policy evaluation. * USE_INVOCATION_RESULT - Applicable if this policy invokes another policy label. If the final goto in the invoked policy label has a value of END, the evaluation stops. If the final goto is anything other than END, the current policy label performs a NEXT. * An expression that evaluates to a number. If you specify an expression, the number to which it evaluates determines the next

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			policy to evaluate, as follows: * If the expression evaluates to a higher numbered priority, the policy with that priority is evaluated next. * If the expression evaluates to the priority of the current policy, the policy with the next higher numbered priority is evaluated next. * If the expression evaluates to a number that is larger than the largest numbered priority, policy evaluation ends. An UNDEF event is triggered if: * The expression is invalid. * The expression evaluates to a priority number that is numerically lower than the current policy's priority. * The expression evaluates to a priority number that is between the current policy's priority number (say, 30) and the highest priority number (say, 100), but does not match any configured priority number (for

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			example, the expression evaluates to the number 85). This example assumes that the priority number increments by 10 for every successive policy, and therefore a priority number of 85 does not exist in the policy label.
policy	<String>	Read-write	The policy Name.
type	<String>	Read-write	Bindpoint to which the policy is bound. Default value: REQUEST Possible values = REQUEST, UDP_REQUEST, DNS_REQUEST, ICMP_REQUEST
priority	<Integer>	Read-write	Integer specifying the priority of the policy. A lower number indicates a higher priority. Policies are evaluated in the order of their priority numbers. Maximum value for default syntax policies is 2147483647 and for classic policies max priority is 64000. .

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum value = 0 Maximum value = 2147483647
username	<String>	Read-write	User account to which to bind the policy. Minimum length = 1
acttype	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/aaauser_auditsyslogpolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"aaauser_auditsyslogpolicy_binding":{

<b>"username":<String_value>,

</b>"policy":<String_value>,

"priority":<Integer_value>,

"type":<String_value>,

"gotopriorityexpression":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaauser_auditsyslogpolicy_binding/ username_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ aaauser_auditsyslogpolicy_binding/ username_value<String> ? **args=policy: <String_value> ,type: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaauser_auditsyslogpolicy_binding/ username_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ aaauser_auditsyslogpolicy_binding/ username_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of aaauser_auditsyslogpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/aaauser_auditsyslogpolicy_binding/ username_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the aaauser_auditsyslogpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "aaauser_auditsyslogpolicy_binding": [ {

"gotopriorityexpression":<String_value>,

"policy":<String_value>,

"type":<String_value>,

"priority":<Integer_value>,

"username":<String_value>,

"acttype":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaauser_auditsyslogpolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/aaauser_auditsyslogpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "aaauser_auditsyslogpolicy_binding": [ {

"gotopriorityexpression":<String_value>,

"policy":<String_value>,

"type":<String_value>,

"priority":<Integer_value>,

"username":<String_value>,

"acttype":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaauser_auditsyslogpolicy_binding/ username_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"aaauser_auditsyslogpolicy_binding": [ { "__count": "#no"} ] }
```

aaauser_authorizationpolicy_binding

Binding object showing the authorizationpolicy that can be bound to aaauser.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
type	<String>	Read-write	Bindpoint to which the policy is bound. Default value: REQUEST Possible values = REQUEST, UDP_REQUEST, DNS_REQUEST, ICMP_REQUEST
username	<String>	Read-write	User account to which to bind the policy. Minimum length = 1
priority	<Integer>	Read-write	Integer specifying the priority of the policy. A lower number indicates a higher priority. Policies are evaluated in the order of their priority numbers. Maximum value for default syntax policies is 2147483647 and for

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			classic policies max priority is 64000. . Minimum value = 0 Maximum value = 2147483647
gotopriorityexpression	<String>	Read-write	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
policy	<String>	Read-write	The policy Name.
acttype	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/aaauser_authorizationpolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"aaauser_authorizationpolicy_binding":{

<b>"username":<String_value>,

</b>"policy":<String_value>,

"priority":<Integer_value>,

"type":<String_value>,
```

```
"gotopriorityexpression":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaauser_authorizationpolicy_binding/ username_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ aaauser_authorizationpolicy_binding/ username_value<String> ? **args=policy: <String_value> ,type: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaauser_authorizationpolicy_binding/ username_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ aaauser_authorizationpolicy_binding/ username_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of aaauser_authorizationpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/aaauser_authorizationpolicy_binding/ username_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the aaauser_authorizationpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "aaauser_authorizationpolicy_binding": [ {

"type":<String_value>,

"username":<String_value>,

"priority":<Integer_value>,

"gotopriorityexpression":<String_value>,

"policy":<String_value>,

"acttype":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaauser_authorizationpolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/aaauser_authorizationpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "aaauser_authorizationpolicy_binding": [ {

"type":<String_value>,

"username":<String_value>,

"priority":<Integer_value>,

"gotopriorityexpression":<String_value>,

"policy":<String_value>,

"acttype":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaauser_authorizationpolicy_binding/username_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"aaauser_authorizationpolicy_binding": [ { "__count": "#no"} ] }
```

aaauser_binding

Binding object which returns the resources bound to aaauser.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
username	<String>	Read-write	Name of the user who has the account. Minimum length = 1
aaauser_vpnurl_binding	<aaauser_vpnurl_binding[]>	Read-only	vpnurl that can be bound to aaauser.
aaauser_vpnurlpolicy_binding	<aaauser_vpnurlpolicy_binding[]>	Read-only	vpnurlpolicy that can be bound to aaauser.
aaauser_vpntrafficpolicy_binding	<aaauser_vpntrafficpolicy_binding[]>	Read-only	vpntrafficpolicy that can be bound to aaauser.
aaauser_tmsessionpolicy_binding	<aaauser_tmsessionpolicy_binding[]>	Read-only	tmsessionpolicy that can be bound to aaauser.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
aaauser_vpnsessionpolicy_binding	<aaauser_vpnsessionpolicy_binding[]>	Read-only	vpnsessionpolicy that can be bound to aaauser.
aaauser_auditsyslogpolicy_binding	<aaauser_auditsyslogpolicy_binding[]>	Read-only	auditsyslogpolicy that can be bound to aaauser.
aaauser_vpnsecureprivateaccessprofile_binding	<aaauser_vpnsecureprivateaccessprofile_binding[]>	Read-only	vpnsecureprivateaccessprofile that can be bound to aaauser.
aaauser_authorizationpolicy_binding	<aaauser_authorizationpolicy_binding[]>	Read-only	authorizationpolicy that can be bound to aaauser.
aaauser_auditnslogpolicy_binding	<aaauser_auditnslogpolicy_binding[]>	Read-only	auditnslogpolicy that can be bound to aaauser.
aaauser_intranetip_binding	<aaauser_intranetip_binding[]>	Read-only	intranetip that can be bound to aaauser.
aaauser_intranetip6_binding	<aaauser_intranetip6_binding[]>	Read-only	intranetip6 that can be bound to aaauser.
aaauser_aaagroup_binding	<aaauser_aaagroup_binding[]>	Read-only	aaagroup that can be bound to aaauser.
aaauser_vpnintranetapplication_binding	<aaauser_vpnintranetapplication_binding[]>	Read-only	vpnintranetapplication that can be bound to aaauser.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaauser_binding/ username_value<String>
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "aaauser_binding": [ {

"username":<String_value>,

"aaauser_intranetip6_binding":<aaauser_intranetip6_binding[]_value>,

"aaauser_vpnurlpolicy_binding":<aaauser_vpnurlpolicy_binding[]_value>,

"aaauser_tmsessionpolicy_binding":<aaauser_tmsessionpolicy_binding[]_value
>,

"aaauser_authorizationpolicy_binding":<aaauser_authorizationpolicy_binding
[]_value>,

"aaauser_vpnurl_binding":<aaauser_vpnurl_binding[]_value>,

"aaauser_aaagroup_binding":<aaauser_aaagroup_binding[]_value>,

"aaauser_vpntrafficpolicy_binding":<aaauser_vpntrafficpolicy_binding[]_val
ue>,

"aaauser_auditnslogpolicy_binding":<aaauser_auditnslogpolicy_binding[]_val
ue>,

"aaauser_vpnintranetapplication_binding":<aaauser_vpnintranetapplication_b
inding[]_value>,

"aaauser_vpnsecureprivateaccessprofile_binding":<aaauser_vpnsecureprivatea
ccessprofile_binding[]_value>,

"aaauser_vpnsessionpolicy_binding":<aaauser_vpnsessionpolicy_binding[]_val
ue>,

"aaauser_auditsyslogpolicy_binding":<aaauser_auditsyslogpolicy_binding[]_v
alue>,

"aaauser_intranetip_binding":<aaauser_intranetip_binding[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaauser_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/aaauser_binding?**bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "aaauser_binding": [ {

"username":<String_value>,

"aaauser_intranetip6_binding":<aaauser_intranetip6_binding[]_value>,

"aaauser_vpnurlpolicy_binding":<aaauser_vpnurlpolicy_binding[]_value>,

"aaauser_tmsessionpolicy_binding":<aaauser_tmsessionpolicy_binding[]_value
>,

"aaauser_authorizationpolicy_binding":<aaauser_authorizationpolicy_binding
[]_value>,

"aaauser_vpnurl_binding":<aaauser_vpnurl_binding[]_value>,

"aaauser_aaagroup_binding":<aaauser_aaagroup_binding[]_value>,
```

```
"aaauser_vpntrafficpolicy_binding":<aaauser_vpntrafficpolicy_binding[]_value>,

"aaauser_auditnslogpolicy_binding":<aaauser_auditnslogpolicy_binding[]_value>,

"aaauser_vpnintranetapplication_binding":<aaauser_vpnintranetapplication_binding[]_value>,

"aaauser_vpnsecureprivateaccessprofile_binding":<aaauser_vpnsecureprivateaccessprofile_binding[]_value>,

"aaauser_vpnsessionpolicy_binding":<aaauser_vpnsessionpolicy_binding[]_value>,

"aaauser_auditsyslogpolicy_binding":<aaauser_auditsyslogpolicy_binding[]_value>,

"aaauser_intranetip_binding":<aaauser_intranetip_binding[]_value>

}]}
```

aaauser_intranetip6_binding

Binding object showing the intranetip6 that can be bound to aaauser.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
gotopriorityexpression	<String>	Read-write	Expression or other value specifying the next policy to evaluate if the current policy evaluates to TRUE. Specify one of the following values: * NEXT - Evaluate the policy with the next

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			higher priority number. * END - End policy evaluation. * USE_INVOCATION_RESULT - Applicable if this policy invokes another policy label. If the final goto in the invoked policy label has a value of END, the evaluation stops. If the final goto is anything other than END, the current policy label performs a NEXT. * An expression that evaluates to a number. If you specify an expression, the number to which it evaluates determines the next policy to evaluate, as follows: * If the expression evaluates to a higher numbered priority, the policy with that priority is evaluated next. * If the expression evaluates to the priority of the current policy, the policy with the next higher numbered priority is evaluated next. * If the expression evaluates to a number that is

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			larger than the largest numbered priority, policy evaluation ends. An UNDEF event is triggered if: * The expression is invalid. * The expression evaluates to a priority number that is numerically lower than the current policy's priority. * The expression evaluates to a priority number that is between the current policy's priority number (say, 30) and the highest priority number (say, 100), but does not match any configured priority number (for example, the expression evaluates to the number 85). This example assumes that the priority number increments by 10 for every successive policy, and therefore a priority number of 85 does not exist in the policy label.
numaddr	<Integer>	Read-write	Numbers of ipv6 address bound starting with intranetip6.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
intranetip6	<String>	Read-write	The Intranet IP6 bound to the user.
username	<String>	Read-write	User account to which to bind the policy. Minimum length = 1
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/aaauser_intranetip6_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"aaauser_intranetip6_binding":{

<b>"username":<String_value>,

</b>"gotopriorityexpression":<String_value>,

"intranetip6":<String_value>,

"numaddr":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaauser_intranetip6_binding/ username_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/

aaauser_intranetip6_binding/ username_value<String> ? **args=intranetip6: <String_value> ,numaddr: <Integer_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaauser_intranetip6_binding/ username_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ aaauser_intranetip6_binding/ username_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of aaauser_intranetip6_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/aaauser_intranetip6_binding/ username_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the aaauser_intranetip6_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "aaauser_intranetip6_binding": [ {

"gotopriorityexpression":<String_value>,

"numaddr":<Integer_value>,

"intranetip6":<String_value>,

"username":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaauser_intranetip6_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/aaauser_intranetip6_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "aaauser_intranetip6_binding": [ {

"gotopriorityexpression":<String_value>,

"numaddr":<Integer_value>,

"intranetip6":<String_value>,

"username":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaauser_intranetip6_binding/ username_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"aaauser_intranetip6_binding": [ { "__count": "#no"} ] }
```

aaauser_intranetip_binding

Binding object showing the intranetip that can be bound to aaauser.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
gotopriorityexpression	<String>	Read-write	Expression or other value specifying the next policy to evaluate if the current policy evaluates to TRUE. Specify one of the following values: * NEXT - Evaluate the policy with the next higher priority number. * END - End policy evaluation. * USE_INVOCATION_RESULT - Applicable if this policy invokes another policy label. If the final goto in the invoked policy label has a value of END, the evaluation stops. If the final goto is anything other than END, the current policy label performs a NEXT. * An expression that evaluates to a number. If you specify an expression, the number to which it evaluates determines the next policy to evaluate, as follows: * If the expression evaluates to a higher numbered priority, the policy with that priority is evaluated

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			next. * If the expression evaluates to the priority of the current policy, the policy with the next higher numbered priority is evaluated next. * If the expression evaluates to a number that is larger than the largest numbered priority, policy evaluation ends. An UNDEF event is triggered if: * The expression is invalid. * The expression evaluates to a priority number that is numerically lower than the current policy's priority. * The expression evaluates to a priority number that is between the current policy's priority number (say, 30) and the highest priority number (say, 100), but does not match any configured priority number (for example, the expression evaluates to the number 85). This example assumes that the priority number increments by 10 for

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			every successive policy, and therefore a priority number of 85 does not exist in the policy label.
username	<String>	Read-write	User account to which to bind the policy. Minimum length = 1
intranetip	<String>	Read-write	The Intranet IP bound to the user.
netmask	<String>	Read-write	The netmask for the Intranet IP.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/aaauser_intranetip_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"aaauser_intranetip_binding":{

<b>"username":<String_value>,

</b>"intranetip":<String_value>,

"netmask":<String_value>,

"gotopriorityexpression":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaauser_intranetip_binding/ username_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ aaauser_intranetip_binding/ username_value<String> ? **args=intranetip: <String_value> ,netmask: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaauser_intranetip_binding/ username_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ aaauser_intranetip_binding/ username_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of aaauser_intranetip_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/aaauser_intranetip_binding/ username_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the aaauser_intranetip_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "aaauser_intranetip_binding": [ {

"gotopriorityexpression":<String_value>,

"username":<String_value>,

"intranetip":<String_value>,

"netmask":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaauser_intranetip_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/aaauser_intranetip_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "aaauser_intranetip_binding": [ {

"gotopriorityexpression":<String_value>,

"username":<String_value>,

"intranetip":<String_value>,

"netmask":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaauser_intranetip_binding/ username_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"aaauser_intranetip_binding": [ { "__count": "#no"} ] }
```

aaauser_tmsessionpolicy_binding

Binding object showing the tmsessionpolicy that can be bound to aaauser.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
type	<String>	Read-write	Bindpoint to which the policy is bound. Default value: REQUEST Possible values = REQUEST, UDP_REQUEST, DNS_REQUEST, ICMP_REQUEST
username	<String>	Read-write	User account to which to bind the policy. Minimum length = 1
priority	<Integer>	Read-write	Integer specifying the priority of the policy. A lower number indicates a higher priority. Policies are evaluated in the order of their priority numbers. Maximum value for default syntax policies is 2147483647 and for

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			classic policies max priority is 64000. . Minimum value = 0 Maximum value = 2147483647
gotopriorityexpression	<String>	Read-write	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
policy	<String>	Read-write	The policy Name.
acttype	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/aaauser_tmsessionpolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"aaauser_tmsessionpolicy_binding":{

<b>"username":<String_value>,

</b>"policy":<String_value>,

"priority":<Integer_value>,

"type":<String_value>,
```

```
"gotopriorityexpression":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaauser_tmsessionpolicy_binding/ username_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ aaauser_tmsessionpolicy_binding/ username_value<String> ? **args=policy: <String_value> ,type: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaauser_tmsessionpolicy_binding/ username_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ aaauser_tmsessionpolicy_binding/ username_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of aaauser_tmsessionpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/aaauser_tmsessionpolicy_binding/ username_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the aaauser_tmsessionpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "aaauser_tmsessionpolicy_binding": [ {

"type":<String_value>,

"username":<String_value>,

"priority":<Integer_value>,

"gotopriorityexpression":<String_value>,

"policy":<String_value>,

"acttype":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaauser_tmsessionpolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/aaauser_tmsessionpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "aaauser_tmsessionpolicy_binding": [ {

"type":<String_value>,

"username":<String_value>,

"priority":<Integer_value>,

"gotopriorityexpression":<String_value>,

"policy":<String_value>,

"acttype":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaauser_tmsessionpolicy_binding/username_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"aaauser_tmsessionpolicy_binding": [ { "__count": "#no"} ] }
```

aaauser_vpnintranetapplication_binding

Binding object showing the vpnintranetapplication that can be bound to aaauser.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
gotopriorityexpression	<String>	Read-write	Expression or other value specifying the next policy to evaluate if the current policy evaluates to TRUE. Specify one of the following values: * NEXT - Evaluate the policy with the next higher priority number. * END - End policy evaluation. * USE_INVOCATION_RESULT - Applicable if this policy invokes another policy label. If the final goto in the invoked policy label has a value of END,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			the evaluation stops. If the final goto is anything other than END, the current policy label performs a NEXT. * An expression that evaluates to a number. If you specify an expression, the number to which it evaluates determines the next policy to evaluate, as follows: * If the expression evaluates to a higher numbered priority, the policy with that priority is evaluated next. * If the expression evaluates to the priority of the current policy, the policy with the next higher numbered priority is evaluated next. * If the expression evaluates to a number that is larger than the largest numbered priority, policy evaluation ends. An UNDEF event is triggered if: * The expression is invalid. * The expression evaluates to a priority number that

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			is numerically lower than the current policy's priority. * The expression evaluates to a priority number that is between the current policy's priority number (say, 30) and the highest priority number (say, 100), but does not match any configured priority number (for example, the expression evaluates to the number 85). This example assumes that the priority number increments by 10 for every successive policy, and therefore a priority number of 85 does not exist in the policy label.
intranetapplication	<String>	Read-write	Name of the intranet VPN application to which the policy applies.
username	<String>	Read-write	User account to which to bind the policy. Minimum length = 1
acttype	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/aaauser_vpnintranetapplication_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"aaauser_vpnintranetapplication_binding":{

<b>"username":<String_value>,

</b>"intranetapplication":<String_value>,

"gotopriorityexpression":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaauser_vpnintranetapplication_binding/ username_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ aaauser_vpnintranetapplication_binding/ username_value<String> ? **args=intranetapplication: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaauser_vpnintranetapplication_binding/ username_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ aaauser_vpnintranetapplication_binding/ username_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of aaauser_vpnintranetapplication_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/aaauser_vpnintranetapplication_binding/ username_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the aaauser_vpnintranetapplication_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "aaauser_vpnintranetapplication_binding": [ {

"gotopriorityexpression":<String_value>,

"intranetapplication":<String_value>,

"username":<String_value>,

"acttype":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaauser_vpnintranetapplication_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/aaauser_vpnintranetapplication_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "aaauser_vpnintranetapplication_binding": [ {

"gotopriorityexpression":<String_value>,

"intranetapplication":<String_value>,

"username":<String_value>,

"acttype":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaauser_vpnintranetapplication_binding/ username_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"aaauser_vpnintranetapplication_binding": [ { "__count": "#no"} ] }
```

aaauser_vpnsecureprivateaccessprofile_binding

Binding object showing the vpnsecureprivateaccessprofile that can be bound to aaauser.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
gotopriorityexpression	<String>	Read-write	Expression or other value specifying the next policy to evaluate if the current policy evaluates to TRUE. Specify one of the following values: * NEXT - Evaluate the policy with the next

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			higher priority number. * END - End policy evaluation. * USE_INVOCATION_RESULT - Applicable if this policy invokes another policy label. If the final goto in the invoked policy label has a value of END, the evaluation stops. If the final goto is anything other than END, the current policy label performs a NEXT. * An expression that evaluates to a number. If you specify an expression, the number to which it evaluates determines the next policy to evaluate, as follows: * If the expression evaluates to a higher numbered priority, the policy with that priority is evaluated next. * If the expression evaluates to the priority of the current policy, the policy with the next higher numbered priority is evaluated next. * If the expression evaluates to a number that is

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			larger than the largest numbered priority, policy evaluation ends. An UNDEF event is triggered if: * The expression is invalid. * The expression evaluates to a priority number that is numerically lower than the current policy's priority. * The expression evaluates to a priority number that is between the current policy's priority number (say, 30) and the highest priority number (say, 100), but does not match any configured priority number (for example, the expression evaluates to the number 85). This example assumes that the priority number increments by 10 for every successive policy, and therefore a priority number of 85 does not exist in the policy label.
secureprivateaccessprofile	<String>	Read-write	Name of the Secure Private Access Profile bound to the user.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
username	<String>	Read-write	User account to which to bind the policy. Minimum length = 1
acttype	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/aaauser_vpnsecureprivateaccessprofile_binding
HTTP Method: PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"aaauser_vpnsecureprivateaccessprofile_binding":{

<b>"username":<String_value>,

</b>"gotopriorityexpression":<String_value>,

"secureprivateaccessprofile":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/ aaauser_vpnsecureprivateaccessprofile_binding/ username_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/

aaauser_vpnsecureprivateaccessprofile_binding/ username_value<String> ? **args=secureprivateaccessprofile: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/ aaauser_vpnsecureprivateaccessprofile_binding/ username_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ aaauser_vpnsecureprivateaccessprofile_binding/ username_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of aaauser_vpnsecureprivateaccessprofile_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ aaauser_vpnsecureprivateaccessprofile_binding/ username_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the aaauser_vpnsecureprivateaccessprofile_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "aaauser_vpnsecureprivateaccessprofile_binding": [ {

"gotopriorityexpression":<String_value>,

"secureprivateaccessprofile":<String_value>,

"username":<String_value>,

"acttype":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/ aaauser_vpnsecureprivateaccessprofile_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ aaauser_vpnsecureprivateaccessprofile_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "aaauser_vpnsecureprivateaccessprofile_binding": [ {

"gotopriorityexpression":<String_value>,

"secureprivateaccessprofile":<String_value>,

"username":<String_value>,

"acttype":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/ aaauser_vpnsecureprivateaccessprofile_binding/ username_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"aaauser_vpnsecureprivateaccessprofile_binding": [ { "__count":
"#no"} ] }
```

aaauser_vpnsessionpolicy_binding

Binding object showing the vpnsessionpolicy that can be bound to aaauser.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
gotopriorityexpression	<String>	Read-write	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
policy	<String>	Read-write	The policy Name.
type	<String>	Read-write	Bindpoint to which the policy is bound. Default value: REQUEST Possible values = REQUEST, UDP_REQUEST, DNS_REQUEST, ICMP_REQUEST
priority	<Integer>	Read-write	Integer specifying the priority of the policy. A lower number indicates a higher priority. Policies are evaluated in the order of their priority numbers. Maximum value for default syntax policies is 2147483647 and for

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			classic policies max priority is 64000. . Minimum value = 0 Maximum value = 2147483647
username	<String>	Read-write	User account to which to bind the policy. Minimum length = 1
acttype	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of

creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/aaauser_vpnsessionpolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"aaauser_vpnsessionpolicy_binding":{

<b>"username":<String_value>,

</b>"policy":<String_value>,

"priority":<Integer_value>,

"type":<String_value>,

"gotopriorityexpression":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaauser_vpnsessionpolicy_binding/ username_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ aaauser_vpnsessionpolicy_binding/ username_value<String> ? **args=policy: <String_value> ,type: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaauser_vpnsessionpolicy_binding/ username_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ aaauser_vpnsessionpolicy_binding/ username_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of aaauser_vpnsessionpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/aaauser_vpnsessionpolicy_binding/ username_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the aaauser_vpnsessionpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "aaauser_vpnsessionpolicy_binding": [ {

"gotopriorityexpression":<String_value>,

"policy":<String_value>,

"type":<String_value>,

"priority":<Integer_value>,

"username":<String_value>,

"acttype":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaauser_vpnsessionpolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/aaauser_vpnsessionpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "aaauser_vpnsessionpolicy_binding": [ {

"gotopriorityexpression":<String_value>,

"policy":<String_value>,

"type":<String_value>,

"priority":<Integer_value>,

"username":<String_value>,

"acttype":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaauser_vpnsessionpolicy_binding/ username_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"aaauser_vpnsessionpolicy_binding": [ { "__count": "#no"} ] }
```

aaauser_vpntrafficpolicy_binding

Binding object showing the vpntrafficpolicy that can be bound to aaauser.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
gotopriorityexpression	<String>	Read-write	Expression or other value specifying the next policy to evaluate if the current policy evaluates to TRUE. Specify one of the following values: * NEXT - Evaluate the policy with the next higher priority number. * END - End policy evaluation. * USE_INVOCATION_RESULT - Applicable if this policy invokes another policy label. If the final goto in the invoked policy label has a value of END, the evaluation stops. If the final goto is anything other than END, the current policy label performs

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			a NEXT. * An expression that evaluates to a number. If you specify an expression, the number to which it evaluates determines the next policy to evaluate, as follows: * If the expression evaluates to a higher numbered priority, the policy with that priority is evaluated next. * If the expression evaluates to the priority of the current policy, the policy with the next higher numbered priority is evaluated next. * If the expression evaluates to a number that is larger than the largest numbered priority, policy evaluation ends. An UNDEF event is triggered if: * The expression is invalid. * The expression evaluates to a priority number that is numerically lower than the current policy's priority. * The expression evaluates to a priority number

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			that is between the current policy's priority number (say, 30) and the highest priority number (say, 100), but does not match any configured priority number (for example, the expression evaluates to the number 85). This example assumes that the priority number increments by 10 for every successive policy, and therefore a priority number of 85 does not exist in the policy label.
policy	<String>	Read-write	The policy Name.
type	<String>	Read-write	Bindpoint to which the policy is bound. Default value: REQUEST Possible values = REQUEST, UDP_REQUEST, DNS_REQUEST, ICMP_REQUEST
username	<String>	Read-write	User account to which to bind the policy. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
priority	<Integer>	Read-write	Integer specifying the priority of the policy. A lower number indicates a higher priority. Policies are evaluated in the order of their priority numbers. Maximum value for default syntax policies is 2147483647 and for classic policies max priority is 64000. . Minimum value = 0 Maximum value = 2147483647
acttype	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/aaauser_vpntrafficpolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"aaauser_vpntrafficpolicy_binding":{

<b>"username":<String_value>,

</b>"policy":<String_value>,

"priority":<Integer_value>,

"type":<String_value>,
```

```
"gotopriorityexpression":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaauser_vpntrafficpolicy_binding/ username_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ aaauser_vpntrafficpolicy_binding/ username_value<String> ? **args=policy: <String_value> ,type: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaauser_vpntrafficpolicy_binding/ username_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ aaauser_vpntrafficpolicy_binding/ username_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of aaauser_vpntrafficpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/aaauser_vpntrafficpolicy_binding/ username_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the aaauser_vpntrafficpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "aaauser_vpntrafficpolicy_binding": [ {

"gotopriorityexpression":<String_value>,

"policy":<String_value>,

"type":<String_value>,

"username":<String_value>,

"priority":<Integer_value>,

"acttype":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaauser_vpntrafficpolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/aaauser_vpntrafficpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "aaauser_vpntrafficpolicy_binding": [ {

"gotopriorityexpression":<String_value>,

"policy":<String_value>,

"type":<String_value>,

"username":<String_value>,

"priority":<Integer_value>,

"acttype":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaauser_vpntrafficpolicy_binding/username_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"aaauser_vpntrafficpolicy_binding": [ { "__count": "#no"} ] }
```

aaauser_vpnurl_binding

Binding object showing the vpnurl that can be bound to aaauser.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
username	<String>	Read-write	User account to which to bind the policy. Minimum length = 1
gotopriorityexpression	<String>	Read-write	Expression or other value specifying the next policy to evaluate if the current policy evaluates to TRUE. Specify one of the following values: * NEXT - Evaluate the policy with the next higher priority number. * END - End policy evaluation. * USE_INVOCATION_RESULT - Applicable

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			if this policy invokes another policy label. If the final goto in the invoked policy label has a value of END, the evaluation stops. If the final goto is anything other than END, the current policy label performs a NEXT. * An expression that evaluates to a number. If you specify an expression, the number to which it evaluates determines the next policy to evaluate, as follows: * If the expression evaluates to a higher numbered priority, the policy with that priority is evaluated next. * If the expression evaluates to the priority of the current policy, the policy with the next higher numbered priority is evaluated next. * If the expression evaluates to a number that is larger than the largest numbered priority, policy evaluation ends. An UNDEF event is

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			triggered if: * The expression is invalid. * The expression evaluates to a priority number that is numerically lower than the current policy's priority. * The expression evaluates to a priority number that is between the current policy's priority number (say, 30) and the highest priority number (say, 100), but does not match any configured priority number (for example, the expression evaluates to the number 85). This example assumes that the priority number increments by 10 for every successive policy, and therefore a priority number of 85 does not exist in the policy label.
urlname	<String>	Read-write	The intranet url.
acttype	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/aaauser_vpnurl_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"aaauser_vpnurl_binding":{

<b>"username":<String_value>,

</b>"urlname":<String_value>,

"gotopriorityexpression":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaauser_vpnurl_binding/ username_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ aaauser_vpnurl_binding/ username_value<String> ? **args=urlname: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaauser_vpnurl_binding/ username_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ aaauser_vpnurl_binding/ username_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of aaauser_vpnurl_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/aaauser_vpnurl_binding/ username_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the aaauser_vpnurl_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "aaauser_vpnurl_binding": [ {

"username":<String_value>,

"gotopriorityexpression":<String_value>,

"urlname":<String_value>,

"acttype":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaauser_vpnurl_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/aaauser_vpnurl_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "aaauser_vpnurl_binding": [ {

"username":<String_value>,

"gotopriorityexpression":<String_value>,

"urlname":<String_value>,

"acttype":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaauser_vpnurl_binding/username_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"aaauser_vpnurl_binding": [ { "__count": "#no"} ] }
```

aaauser_vpnurlpolicy_binding

Binding object showing the vpnurlpolicy that can be bound to aaauser.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
policy	<String>	Read-write	The policy Name.
gotopriorityexpression	<String>	Read-write	Expression or other value specifying the next policy to evaluate if the current policy evaluates to TRUE. Specify one of the following values: * NEXT - Evaluate the policy with the next higher priority number. * END - End policy evaluation. * USE_INVOCATION_RESULT - Applicable if this policy invokes another policy label. If the final goto in the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			invoked policy label has a value of END, the evaluation stops. If the final goto is anything other than END, the current policy label performs a NEXT. * An expression that evaluates to a number. If you specify an expression, the number to which it evaluates determines the next policy to evaluate, as follows: * If the expression evaluates to a higher numbered priority, the policy with that priority is evaluated next. * If the expression evaluates to the priority of the current policy, the policy with the next higher numbered priority is evaluated next. * If the expression evaluates to a number that is larger than the largest numbered priority, policy evaluation ends. An UNDEF event is triggered if: * The expression is invalid. * The expression

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			evaluates to a priority number that is numerically lower than the current policy's priority. * The expression evaluates to a priority number that is between the current policy's priority number (say, 30) and the highest priority number (say, 100), but does not match any configured priority number (for example, the expression evaluates to the number 85). This example assumes that the priority number increments by 10 for every successive policy, and therefore a priority number of 85 does not exist in the policy label.
priority	<Integer>	Read-write	Integer specifying the priority of the policy. A lower number indicates a higher priority. Policies are evaluated in the order of their priority numbers. Maximum value for default syntax policies is 2147483647 and for

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			classic policies max priority is 64000. . Minimum value = 0 Maximum value = 2147483647
username	<String>	Read-write	User account to which to bind the policy. Minimum length = 1
type	<String>	Read-write	Bindpoint to which the policy is bound. Default value: REQUEST Possible values = REQUEST, UDP_REQUEST, DNS_REQUEST, ICMP_REQUEST
acttype	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/aaauser_vpnurlpolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"aaauser_vpnurlpolicy_binding":{

<b>"username":<String_value>,
```

```
</b>"policy":<String_value>,

"priority":<Integer_value>,

"type":<String_value>,

"gotopriorityexpression":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaauser_vpnurlpolicy_binding/ username_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ aaauser_vpnurlpolicy_binding/ username_value<String> ? **args=policy: <String_value> ,type: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaauser_vpnurlpolicy_binding/ username_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ aaauser_vpnurlpolicy_binding/ username_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of aaauser_vpnurlpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/aaauser_vpnurlpolicy_binding/ username_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the aaauser_vpnurlpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "aaauser_vpnurlpolicy_binding": [ {

"policy":<String_value>,

"gotopriorityexpression":<String_value>,

"priority":<Integer_value>,

"username":<String_value>,

"type":<String_value>,

"acttype":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaauser_vpnurlpolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/aaauser_vpnurlpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "aaauser_vpnurlpolicy_binding": [ {

"policy":<String_value>,

"gotopriorityexpression":<String_value>,

"priority":<Integer_value>,

"username":<String_value>,

"type":<String_value>,

"acttype":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/aaauser_vpnurlpolicy_binding/username_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"aaauser_vpnurlpolicy_binding": [ { "__count": "#no"} ] }
```

adm

Adm

ADM related configuration.

NAME	DESCRIPTION
admparameter	Configuration for ADM parameter

admparameter

Configuration for ADM parameter resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
admserviceconnect	<String>	Read-write	Parameter to enable/ disable Citrix ADM Service Connect. This feature helps

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			you discover your Citrix ADC instances effortlessly on Citrix ADM service and get insights and curated machine learning based recommendations for applications and Citrix ADC infrastructure. This feature lets the Citrix ADC instance automatically send system, usage and telemetry data to Citrix ADM service. View here [https://docs.citrix.com/en-us/citrix-adc/13/data-governance.html] to learn more about this feature. Use of this feature is subject to the Citrix End User ServiceAgreement. View here [https://www.citrix.com/buy/licensing/agreements.html]. Default value: ENABLED Possible values = ENABLED, DISABLED
lowtouchonboard	<String>	Read-only	ENABLED value indicates that this ADC can be on-boarded onto Citrix

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			ADM Service using auto-onboarding process. Refer to [https://docs.citrix.com/en-us/citrix-application-delivery-management-service/service-connect-onboarding.html] for further details. Possible values = ENABLED, DISABLED
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- UPDATE
- UNSET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of

creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/admparameter **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"admparameter":{

"admserviceconnect":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/admparameter? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"admparameter":{

"admserviceconnect":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/admparameter **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "admparameter": [ {

"admserviceconnect":<String_value>,

"lowtouchonboard":<String_value>,
```

```
"_nextgenapiresource":<String_value>

}]}
```

analytics

Analytics

Analytics configuration.

NAME	DESCRIPTION
analyticsglobal_analyticsprofile_binding	Binding object showing the analyticsprofile that can be bound to analyticsglobal
analyticsglobal_binding	Binding object showing the resources that can be bound to analyticsglobal
analyticsprofile	Configuration for Analytics profile

analyticsglobal_analyticsprofile_binding

Binding object showing the analyticsprofile that can be bound to analyticsglobal.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
analyticsprofile	<String>	Read-write	Name of the analytics profile bound.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/analyticsglobal_analyticsprofile_binding

HTTP Method: PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"analyticsglobal_analyticsprofile_binding":{

<b>"analyticsprofile":<String_value></b>

}}
```

Response:

HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/analyticsglobal_analyticsprofile_binding

Query-parameters:

args

http:// <netscaler-ip-address> /nitro/v1/config/analyticsglobal_analyticsprofile_binding? **args= analyticsprofile:<String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/analyticsglobal_analyticsprofile_binding

Query-parameters:

filter

http:// <netscaler-ip-address> /nitro/v1/config/analyticsglobal_analyticsprofile_binding?**filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of analyticsglobal_analyticsprofile_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination

http:// <netscaler-ip-address> /nitro/v1/config/analyticsglobal_analyticsprofile_binding?**pagesize=#no;pageno=#no**

Use this query-parameter to get the analyticsglobal_analyticsprofile_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "analyticsglobal_analyticsprofile_binding": [ {

"analyticsprofile":<String_value>
```

```
}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/analyticsglobal_analyticsprofile_binding?**count=yes**

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "analyticsglobal_analyticsprofile_binding": [ { "__count": "#no"} ] }
```

analyticsglobal_binding

Binding object which returns the resources bound to analyticsglobal.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
analyticsglobal_analyticsprofile_binding	<analyticsglobal_analyticsprofile_binding[]>	Read-write	analyticsprofile that can be bound to analyticsglobal.

Operations

(click to see Properties)

- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/analyticsglobal_binding

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "analyticsglobal_binding": [ {

"analyticsglobal_analyticsprofile_binding":<analyticsglobal_analyticsprofi
le_binding[]_value>

}]}
```

analyticsprofile

Configuration for Analytics profile resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the analytics profile. Must begin with an ASCII alphabetic or underscore (_) character, and must

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my appflow profile" or 'my appflow profile'). Minimum length = 1 Maximum length = 127
collectors	<String>	Read-write	The collector can be an IP, an appflow collector name, a service or a vserver. If IP is specified, the transport is considered as logstream and default port of 5557 is taken. If collector name is specified,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			the collector properties are taken from the configured collector. If service is specified, the configured service is assumed as the collector. If vserver is specified, the services bound to it are considered as collectors and the records are load balanced. Minimum length = 1
type	<String>	Read-write	This option indicates what information needs to be collected and exported. Possible values = global, webinsight, tcpinsight, securityinsight, videoinsight, hdxinsight, gatewayinsight, timeseries, lsninsight, botinsight, CIinsight, udpinsight, ngsinsight, streaminsight
httpclientsidemeasurements	<String>	Read-write	On enabling this option, the Citrix ADC will insert a javascript into the HTTP response to

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			collect the client side page-timings and will send the same to the configured collectors. Default value: DISABLED Possible values = ENABLED, DISABLED
httppagetracking	<String>	Read-write	On enabling this option, the Citrix ADC will link the embedded objects of a page together. Default value: DISABLED Possible values = ENABLED, DISABLED
httpurl	<String>	Read-write	On enabling this option, the Citrix ADC will log the URL in appflow records. Default value: DISABLED Possible values = ENABLED, DISABLED
httphost	<String>	Read-write	On enabling this option, the Citrix ADC will log the Host header in appflow records.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: DISABLED Possible values = ENABLED, DISABLED
httpmethod	<String>	Read-write	On enabling this option, the Citrix ADC will log the method header in appflow records. Default value: DISABLED Possible values = ENABLED, DISABLED
httpreferer	<String>	Read-write	On enabling this option, the Citrix ADC will log the referer header in appflow records. Default value: DISABLED Possible values = ENABLED, DISABLED
httpuseragent	<String>	Read-write	On enabling this option, the Citrix ADC will log User-Agent header. Default value: DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ENABLED, DISABLED
httpcookie	<String>	Read-write	On enabling this option, the Citrix ADC will log cookie header. Default value: DISABLED Possible values = ENABLED, DISABLED
httplocation	<String>	Read-write	On enabling this option, the Citrix ADC will log location header. Default value: DISABLED Possible values = ENABLED, DISABLED
urlcategory	<String>	Read-write	On enabling this option, the Citrix ADC will send the URL category record. Default value: DISABLED Possible values = ENABLED, DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
allhttpheaders	<String>	Read-write	On enabling this option, the Citrix ADC will log all the request and response headers. Default value: DISABLED Possible values = ENABLED, DISABLED
httpcontenttype	<String>	Read-write	On enabling this option, the Citrix ADC will log content-length header. Default value: DISABLED Possible values = ENABLED, DISABLED
httpauthentication	<String>	Read-write	On enabling this option, the Citrix ADC will log Authentication header. Default value: DISABLED Possible values = ENABLED, DISABLED
httpvia	<String>	Read-write	On enabling this option, the Citrix ADC will Via header.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: DISABLED Possible values = ENABLED, DISABLED
httpxforwardedforheader	<String>	Read-write	On enabling this option, the Citrix ADC will log X-Forwarded-For header. Default value: DISABLED Possible values = ENABLED, DISABLED
httpsetcookie	<String>	Read-write	On enabling this option, the Citrix ADC will log set-cookie header. Default value: DISABLED Possible values = ENABLED, DISABLED
httpsetcookie2	<String>	Read-write	On enabling this option, the Citrix ADC will log set-cookie2 header. Default value: DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ENABLED, DISABLED
httpdomainname	<String>	Read-write	On enabling this option, the Citrix ADC will log domain name. Default value: DISABLED Possible values = ENABLED, DISABLED
httpurlquery	<String>	Read-write	On enabling this option, the Citrix ADC will log URL Query. Default value: DISABLED Possible values = ENABLED, DISABLED
tcpburstreporting	<String>	Read-write	On enabling this option, the Citrix ADC will log TCP burst parameters. Default value: ENABLED Possible values = ENABLED, DISABLED
cqareporting	<String>	Read-write	On enabling this option, the Citrix

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			ADC will log TCP CQA parameters. Default value: DISABLED Possible values = ENABLED, DISABLED
integratedcache	<String>	Read-write	On enabling this option, the Citrix ADC will log the Integrated Caching appflow records. Default value: DISABLED Possible values = ENABLED, DISABLED
grpcstatus	<String>	Read-write	On enabling this option, the Citrix ADC will log the gRPC status headers. Default value: DISABLED Possible values = ENABLED, DISABLED
outputmode	<String>	Read-write	This option indicates the format of REST API POST body. It depends on the consumer of the analytics data.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: avro, Possible values = avro, prometheus, influx, json
metrics	<String>	Read-write	This option indicates the whether metrics should be sent to the REST collector. Default value: DISABLED Possible values = ENABLED, DISABLED
events	<String>	Read-write	This option indicates the whether events should be sent to the REST collector. Default value: DISABLED Possible values = ENABLED, DISABLED
auditlogs	<String>	Read-write	This option indicates the whether auditlog should be sent to the REST collector. Default value: DISABLED Possible values = ENABLED, DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
servemode	<String>	Read-write	This option is for setting the mode of how data is provided. Default value: Push Possible values = Push, Pull
schemafile	<String>	Read-write	This option is for configuring json schema file containing a list of counters to be exported by metricscollector. Maximum length = 64
metricsexportfrequency	<Integer>	Read-write	This option is for configuring the metrics export frequency in seconds, frequency value must be in [30,300] seconds range. Default value: 30 Minimum value = 30 Maximum value = 300
analyticsendpointmetadata	<String>	Read-write	If the endpoint requires some metadata to be present before the actual json data, specify the same.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum length = 128
dataformatfile	<String>	Read-write	This option is for configuring the file containing the data format and metadata required by the analytics endpoint. Note that the fields to be exported will be honoured only if the option logAllJsonFields is disabled under appflow param. Maximum length = 64
topn	<String>	Read-write	On enabling this topn support, the topn information of the stream identifier this profile is bound to will be exported to the analytics endpoint. Default value: DISABLED Possible values = ENABLED, DISABLED
httpcustomheaders	<String[]>	Read-write	Specify the list of custom headers to be exported in web transaction records. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
mcpsummary	<String>	Read-write	Enable/disable appflow logging for MCP (Model Context Protocol) traffic. Default value: DISABLED Possible values = ENABLED, DISABLED
managementlog	<String[]>	Read-write	This option indicates the whether managementlog should be sent to the REST collector. Default value: DEFAULT_MANAGEMENTLOG Possible values = ALL, SHELL, ACCESS, NSMGMT, NONE
analyticsauthtoken	<String>	Read-write	Token for authenticating with the endpoint. If the endpoint requires the Authorization header in a particular format, specify the complete format as the value to this parameter. For eg., in case of splunk, the Authorizaiton header is required to be of

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			the form - Splunk <auth-token>. Maximum length = 512
analyticsendpointurl	<String>	Read-write	The URL at which to upload the analytics data on the endpoint. Maximum length = 256
analyticsendpointcontenttype	<String>	Read-write	By default, application/json content-type is used. If this needs to be overridden, specify the value. Maximum length = 128
refcnt	<Integer>	Read-only	The number of references to the profile.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- UPDATE
- UNSET
- DELETE
- GET (ALL)
- GET

- COUNT
- CHANGE

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/analyticsprofile **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"analyticsprofile":{

<b>"name":<String_value>,

</b>"collectors":<String_value>,

<b>"type":<String_value>,

</b>"httpclientsidemeasurements":<String_value>,

"httppagetracking":<String_value>,

"httpurl":<String_value>,

"httphost":<String_value>,

"httpmethod":<String_value>,

"httpreferer":<String_value>,

"httpuseragent":<String_value>,

"httpcookie":<String_value>,

"httplocation":<String_value>,

"urlcategory":<String_value>,

"allhttpheaders":<String_value>,

"httpcontenttype":<String_value>,

"httpauthentication":<String_value>,

"httpvia":<String_value>,

"httpxforwardedforheader":<String_value>,

"httpsetcookie":<String_value>,

"httpsetcookie2":<String_value>,

"httpdomainname":<String_value>,
```

```
"httpurlquery":<String_value>,

"tcpburstreporting":<String_value>,

"cqareporting":<String_value>,

"integratedcache":<String_value>,

"grpcstatus":<String_value>,

"outputmode":<String_value>,

"metrics":<String_value>,

"events":<String_value>,

"auditlogs":<String_value>,

"servemode":<String_value>,

"schemafile":<String_value>,

"metricsexportfrequency":<Integer_value>,

"analyticsendpointmetadata":<String_value>,

"dataformatfile":<String_value>,

"topn":<String_value>,

"httpcustomheaders":<String[]_value>,

"mcpsummary":<String_value>,

"managementlog":<String[]_value>,

"analyticsauthtoken":<String_value>,

"analyticsendpointurl":<String_value>,

"analyticsendpointcontenttype":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/analyticsprofile **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"analyticsprofile":{

<b>"name":<String_value>,

</b>"collectors":<String_value>,

"type":<String_value>,

"httpclientsidemeasurements":<String_value>,

"httppagetracking":<String_value>,

"httpurl":<String_value>,

"httphost":<String_value>,

"httpmethod":<String_value>,

"httpreferer":<String_value>,

"httpuseragent":<String_value>,

"httpcookie":<String_value>,

"httplocation":<String_value>,
```

```
"urlcategory":<String_value>,

"allhttpheaders":<String_value>,

"httpcontenttype":<String_value>,

"httpauthentication":<String_value>,

"httpvia":<String_value>,

"httpxforwardedforheader":<String_value>,

"httpsetcookie":<String_value>,

"httpsetcookie2":<String_value>,

"httpdomainname":<String_value>,

"httpurlquery":<String_value>,

"tcpburstreporting":<String_value>,

"cqareporting":<String_value>,

"integratedcache":<String_value>,

"grpcstatus":<String_value>,

"outputmode":<String_value>,

"metrics":<String_value>,

"events":<String_value>,

"auditlogs":<String_value>,

"managementlog":<String[]_value>,

"servemode":<String_value>,

"schemafile":<String_value>,

"metricsexportfrequency":<Integer_value>,
```

```
"analyticsauthtoken":<String_value>,

"analyticsendpointurl":<String_value>,

"analyticsendpointcontenttype":<String_value>,

"analyticsendpointmetadata":<String_value>,

"dataformatfile":<String_value>,

"topn":<String_value>,

"httpcustomheaders":<String[]_value>,

"mcpsummary":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/analyticsprofile? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"analyticsprofile":{

<b>"name":<String_value>,

</b>"collectors":true,
```

```
"type":true,

"httpclientsidemeasurements":true,

"httppagetracking":true,

"httpurl":true,

"httphost":true,

"httpmethod":true,

"httpreferer":true,

"httpuseragent":true,

"httpcookie":true,

"httplocation":true,

"urlcategory":true,

"allhttpheaders":true,

"httpcontenttype":true,

"httpauthentication":true,

"httpvia":true,

"httpxforwardedforheader":true,

"httpsetcookie":true,

"httpsetcookie2":true,

"httpdomainname":true,

"httpurlquery":true,

"tcpburstreporting":true,

"cqareporting":true,
```

```
"integratedcache":true,

"grpcstatus":true,

"outputmode":true,

"metrics":true,

"events":true,

"auditlogs":true,

"managementlog":true,

"servemode":true,

"schemafile":true,

"metricsexportfrequency":true,

"analyticsauthtoken":true,

"analyticsendpointurl":true,

"analyticsendpointcontenttype":true,

"analyticsendpointmetadata":true,

"dataformatfile":true,

"topn":true,

"httpcustomheaders":true,

"mcpsummary":true

}}
```


Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/analyticsprofile/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

CHANGE

URL: http:// <netscaler-ip-address> /nitro/v1/config/analyticsprofile? **action=update HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"analyticsprofile":{

<b>"name":<String_value>,

</b>"dataformatfile":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/analyticsprofile **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/analyticsprofile? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/analyticsprofile? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of analyticsprofile resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/analyticsprofile? **view=summary**

Use this query-parameter to get the summary output of analyticsprofile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/analyticsprofile? **pagesize=#no;pageno=#no**

Use this query-parameter to get the analyticsprofile resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "analyticsprofile": [ {

"name":<String_value>,

"collectors":<String_value>,

"refcnt":<Integer_value>,

"type":<String_value>,

"httpclientsidemeasurements":<String_value>,

"httppagetracking":<String_value>,

"httpurl":<String_value>,

"httphost":<String_value>,

"httpmethod":<String_value>,

"httpreferer":<String_value>,

"httpuseragent":<String_value>,

"httpcookie":<String_value>,

"httplocation":<String_value>,

"urlcategory":<String_value>,

"allhttpheaders":<String_value>,

"httpcontenttype":<String_value>,

"httpauthentication":<String_value>,

"httpvia":<String_value>,

"httpxforwardedforheader":<String_value>,

"httpsetcookie":<String_value>,

"httpsetcookie2":<String_value>,
```

```
"httpdomainname":<String_value>,

"httpurlquery":<String_value>,

"tcpburstreporting":<String_value>,

"cqareporting":<String_value>,

"integratedcache":<String_value>,

"grpcstatus":<String_value>,

"outputmode":<String_value>,

"metrics":<String_value>,

"events":<String_value>,

"auditlogs":<String_value>,

"managementlog":<String[]_value>,

"servemode":<String_value>,

"schemafile":<String_value>,

"metricsexportfrequency":<Integer_value>,

"analyticsauthtoken":<String_value>,

"analyticsendpointurl":<String_value>,

"analyticsendpointcontenttype":<String_value>,

"analyticsendpointmetadata":<String_value>,

"dataformatfile":<String_value>,

"topn":<String_value>,

"httpcustomheaders":<String[]_value>,

"mcpsummary":<String_value>,
```

```
"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/analyticsprofile/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/analyticsprofile/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/analyticsprofile/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of analyticsprofile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "analyticsprofile": [ {

"name":<String_value>,
```

```
"collectors":<String_value>,

"refcnt":<Integer_value>,

"type":<String_value>,

"httpclientsidemeasurements":<String_value>,

"httppagetracking":<String_value>,

"httpurl":<String_value>,

"httphost":<String_value>,

"httpmethod":<String_value>,

"httpreferer":<String_value>,

"httpuseragent":<String_value>,

"httpcookie":<String_value>,

"httplocation":<String_value>,

"urlcategory":<String_value>,

"allhttpheaders":<String_value>,

"httpcontenttype":<String_value>,

"httpauthentication":<String_value>,

"httpvia":<String_value>,

"httpxforwardedforheader":<String_value>,

"httpsetcookie":<String_value>,

"httpsetcookie2":<String_value>,

"httpdomainname":<String_value>,

"httpurlquery":<String_value>,
```

```
"tcpburstreporting":<String_value>,

"cqareporting":<String_value>,

"integratedcache":<String_value>,

"grpcstatus":<String_value>,

"outputmode":<String_value>,

"metrics":<String_value>,

"events":<String_value>,

"auditlogs":<String_value>,

"managementlog":<String[]_value>,

"servemode":<String_value>,

"schemafile":<String_value>,

"metricsexportfrequency":<Integer_value>,

"analyticsauthtoken":<String_value>,

"analyticsendpointurl":<String_value>,

"analyticsendpointcontenttype":<String_value>,

"analyticsendpointmetadata":<String_value>,

"dataformatfile":<String_value>,

"topn":<String_value>,

"httpcustomheaders":<String[]_value>,

"mcpsummary":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

```
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/analyticsprofile? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "analyticsprofile": [ { "__count": "#no"} ] }
```

api

Api

API Configuration

NAME	DESCRIPTION
apiprofile	Configuration for API profile
apiprofile_apispec_binding	Binding object showing the apispec that can be bound to apiprofile

NAME	DESCRIPTION
apiprofile_binding	Binding object showing the resources that can be bound to apiprofile
apispec	Configuration for API specification
apispec_binding	Binding object showing the resources that can be bound to apispec
apispec_specendpoint_binding	Binding object showing the specendpoint that can be bound to apispec
apispecfile	Configuration for API specification file

apiprofile

Configuration for API profile resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the API profile to add. Minimum length = 1
apivisibility	<String>	Read-write	Enable/Disable the schema lookup for the requests/ apispecs that are bounded to the API profile. The default value of this parameter is DISABLED.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: DISABLED Possible values = ENABLED, DISABLED
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET (ALL)
- GET
- COUNT
- UPDATE
- UNSET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/apiprofile **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"apiprofile":{

<b>"name":<String_value>,

</b>"apivisibility":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/apiprofile/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/apiprofile **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"apiprofile":{

<b>"name":<String_value>,

</b>"apivisibility":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/apiprofile? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"apiprofile":{

<b>"name":<String_value>,

</b>"apivisibility":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/apiprofile **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/apiprofile? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/apiprofile? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of apiprofile resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/apiprofile? **view=summary**

Use this query-parameter to get the summary output of apiprofile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/apiprofile? **pagesize=#no;pageno=#no**

Use this query-parameter to get the apiprofile resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "apiprofile": [ {

"name":<String_value>,

"apivisibility":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/apiprofile/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/apiprofile/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/apiprofile/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of apiprofile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "apiprofile": [ {

"name":<String_value>,

"apivisibility":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/apiprofile? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "apiprofile": [ { "__count": "#no"} ] }
```

apiprofile_apispec_binding

Binding object showing the apispec that can be bound to apiprofile.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
apispec	<String>	Read-write	Name for the API spec which will be binded to the profile. Minimum length = 1
name	<String>	Read-write	Name of the API profile in which to bind the API apispec(s). Minimum length = 1
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT
- ADD
- DELETE

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/apiprofile_apispec_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"apiprofile_apispec_binding":{

<b>"name":<String_value>,

</b><b>"apispec":<String_value></b>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/apiprofile_apispec_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ apiprofile_apispec_binding/ name_value<String> ? **args= apispec:<String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/apiprofile_apispec_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ apiprofile_apispec_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of apiprofile_apispec_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/apiprofile_apispec_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the apiprofile_apispec_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "apiprofile_apispec_binding": [ {

"apispec":<String_value>,

"name":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/apiprofile_apispec_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/apiprofile_apispec_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "apiprofile_apispec_binding": [ {

"apispec":<String_value>,

"name":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/apiprofile_apispec_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"apiprofile_apispec_binding": [ { "__count": "#no"} ] }
```

apiprofile_binding

Binding object which returns the resources bound to apiprofile.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the API profile. Minimum length = 1
apiprofile_apispec_binding	<apiprofile_apispec_binding[]>	Read-only	apispec that can be bound to apiprofile.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/apiprofile_binding/ name_value<String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "apiprofile_binding": [ {

"name":<String_value>,

"apiprofile_apispec_binding":<apiprofile_apispec_binding[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/apiprofile_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ apiprofile_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "apiprofile_binding": [ {

"name":<String_value>,

"apiprofile_apispec_binding":<apiprofile_apispec_binding[]_value>

}]}
```

apispec

Configuration for API specification resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the spec. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			characters. Cannot be changed after the spec is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my spec" or 'my spec'). Minimum length = 1
file	<String>	Read-write	Name of and, optionally, path to the api spec file. The spec file should be present on the appliance's hard-disk drive or solid-state drive. Storing a spec file in any location other than the default might cause inconsistency in a high availability setup. /nsconfig/apispec/ is the default path. Minimum length = 1
type	<String>	Read-write	Input format of the spec file. The three

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			formats supported by the appliance are: PROTO OAS/Swagger GRAPHQL. Default value: OAS Possible values = PROTO, OAS, GRAPHQL
skipvalidation	<String>	Read-write	Disabling openapi spec validation while adding it. Default value: NO Possible values = YES, NO
encrypted	<Boolean>	Read-write	Specify the encrypted API spec. Must be in NetScaler format.
builtin	<String[]>	Read-only	. Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL
ready	<String>	Read-only	Indicates whether apec is ready, that is internal registry created or not. Default value: NO

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = YES, NO
nsappversion	<String>	Read-only	NS App Version of the api spec file.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- GET (ALL)
- GET
- COUNT
- DELETE
- CHANGE

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/apispec **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"apispec":{

<b>"name":<String_value>,

</b><b>"file":<String_value>,

</b>"type":<String_value>,

"skipvalidation":<String_value>,

"encrypted":<Boolean_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/apispec/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

CHANGE

URL: http:// <netscaler-ip-address> /nitro/v1/config/apispec? **action=update HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"apispec":{

<b>"name":<String_value>,

</b><b>"file":<String_value>,

</b>"type":<String_value>,

"skipvalidation":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/apispec **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/apispec? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/apispec? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of apispec resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/apispec? **view=summary**

Use this query-parameter to get the summary output of apispec resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/apispec? **pagesize=#no;pageno=#no**

Use this query-parameter to get the apispec resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "apispec": [ {

"name":<String_value>,

"file":<String_value>,

"type":<String_value>,

"skipvalidation":<String_value>,
```

```
"encrypted":<Boolean_value>,

"builtin":<String[]_value>,

"ready":<String_value>,

"nsappversion":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/apispec/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/apispec/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/apispec/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of apispec resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "apispec": [ {

"name":<String_value>,

"file":<String_value>,

"type":<String_value>,

"skipvalidation":<String_value>,

"encrypted":<Boolean_value>,

"builtin":<String[]_value>,

"ready":<String_value>,

"nsappversion":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/apispec? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "apispec": [ { "__count": "#no"} ] }
```

apispec_binding

Binding object which returns the resources bound to apispec.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the spec for which to show detailed information. Minimum length = 1
apispec_specendpoint_binding	<apispec_specendpoint_binding[]>	Read-only	specendpoint that can be bound to apispec.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/apispec_binding/ name_value<String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "apispec_binding": [ {

"name":<String_value>,

"apispec_specendpoint_binding":<apispec_specendpoint_binding[]_value>
```

```
}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/apispec_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/apispec_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "apispec_binding": [ {

"name":<String_value>,

"apispec_specendpoint_binding":<apispec_specendpoint_binding[]_value>

}]}
```

apispec_specendpoint_binding

Binding object showing the specendpoint that can be bound to apispec.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
apiname	<String>	Read-write	API method used for display purposes.
name	<String>	Read-write	Name of the spec for which to show detailed information. Minimum length = 1
httpmethod	<String>	Read-only	GRPC API option method: REST way to reach GRPC Service. One per service/method combination.
apiservice	<String>	Read-only	API endpoint (could be GRPC service, REST path) used for display purposes.
httpurlpath	<String>	Read-only	GRPC API option endpoint: REST way to reach GRPC Service. One per service/method combination.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/apispec_specendpoint_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ apispec_specendpoint_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of apispec_specendpoint_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/apispec_specendpoint_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the apispec_specendpoint_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "apispec_specendpoint_binding": [ {

"apiname":<String_value>,

"name":<String_value>,

"httpmethod":<String_value>,

"apiservice":<String_value>,

"httpurlpath":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/apispec_specendpoint_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/apispec_specendpoint_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "apispec_specendpoint_binding": [ {

"apiname":<String_value>,

"name":<String_value>,

"httpmethod":<String_value>,

"apiservice":<String_value>,

"httpurlpath":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/apispec_specendpoint_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"apispec_specendpoint_binding": [ { "__count": "#no"} ] }
```

apispecfile

Configuration for API specification file resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name to assign to the imported spec file. Must begin with an ASCII alphanumeric or underscore(_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@),equals (=), and hyphen (-) characters. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my file" or 'my file').

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum length = 1 Maximum length = 31
src	<String>	Read-write	URL specifying the protocol, host, and path, including file name, to the spec file to be imported. For example, http://www.example.com/spec_file. NOTE: The import fails if the object to be imported is on an HTTPS server that requires client certificate authentication for access. Minimum length = 1 Maximum length = 2047
overwrite	<Boolean>	Read-write	Overwrite any existing schema file of the same name.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- IMPORT

- DELETE
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

IMPORT

URL: http:// <netscaler-ip-address> /nitro/v1/config/apispecfile? **action=Import HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"apispecfile":{

<b>"name":<String_value>,

</b><b>"src":<String_value>,

</b>"overwrite":<Boolean_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/apispecfile/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/apispecfile **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/apispecfile? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/apispecfile? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of apispecfile resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/apispecfile? **view=summary**

Use this query-parameter to get the summary output of apispecfile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/apispecfile? **pagesize=#no;pageno=#no**

Use this query-parameter to get the apispecfile resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "apispecfile": [ {

"name":<String_value>,

"src":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/apispecfile? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "apispecfile": [ { "__count": "#no"} ] }
```

app

App

Application

NAME	DESCRIPTION
application	Configuration for application

application

Configuration for application resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
apptemplatefilename	<String>	Read-write	Name of the AppExpert application template file.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
appname	<String>	Read-write	Name to assign to the application on the Citrix ADC. If you do not provide a name, the appliance assigns the application the name of the template file.
deploymentfilename	<String>	Read-write	Name of the deployment file.

Operations

(click to see Properties)

- IMPORT
- EXPORT
- DELETE

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

IMPORT

URL: http:// <netscaler-ip-address> /nitro/v1/config/application? **action=Import**

HTTP Method: POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"application":{

<b>"apptemplatefilename":<String_value>,

</b>"appname":<String_value>,

"deploymentfilename":<String_value>

}}
```

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

EXPORT

URL: http:// <netscaler-ip-address> /nitro/v1/config/application? **action=export**

HTTP Method: POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"application":{

<b>"appname":<String_value>,

</b>"apptemplatefilename":<String_value>,

"deploymentfilename":<String_value>

}}
```

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/application

Query-parameters:

args= appname:<String_value>

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

appflow

Appflow

AppFlow configuration.

NAME	DESCRIPTION
appflowaction	Configuration for AppFlow action
appflowaction_analyticsprofile_binding	Binding object showing the analyticsprofile that can be bound to appflowaction
appflowaction_binding	Binding object showing the resources that can be bound to appflowaction
appflowcollector	Configuration for AppFlow collector
appflowglobal_appflowpolicy_binding	Binding object showing the appflowpolicy that can be bound to appflowglobal
appflowglobal_binding	Binding object showing the resources that can be bound to appflowglobal
appflowparam	Configuration for AppFlow parameter
appflowpolicy	Configuration for AppFlow policy
appflowpolicy_appflowglobal_binding	Binding object showing the appflowglobal that can be bound to appflowpolicy

NAME	DESCRIPTION
appflowpolicy_appflowpolicylabel_binding	Binding object showing the appflowpolicylabel that can be bound to appflowpolicy
appflowpolicy_binding	Binding object showing the resources that can be bound to appflowpolicy
appflowpolicy_csvserver_binding	Binding object showing the csvserver that can be bound to appflowpolicy
appflowpolicy_lbvserver_binding	Binding object showing the lbvserver that can be bound to appflowpolicy
appflowpolicy_vpnvserver_binding	Binding object showing the vpnvserver that can be bound to appflowpolicy
appflowpolicylabel	Configuration for AppFlow policy label
appflowpolicylabel_appflowpolicy_binding	Binding object showing the appflowpolicy that can be bound to appflowpolicylabel
appflowpolicylabel_binding	Binding object showing the resources that can be bound to appflowpolicylabel

appflowaction

Configuration for AppFlow action resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the action. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my appflow action" or 'my appflow action').
collectors	<String[]>	Read-write	Name(s) of collector(s) to be associated with the AppFlow action. Minimum length = 1
clientsidemeasurements	<String>	Read-write	On enabling this option, the Citrix ADC will collect the time required to load and render the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			mainpage on the client. Default value: DISABLED Possible values = ENABLED, DISABLED
pagetracking	<String>	Read-write	On enabling this option, the Citrix ADC will start tracking the page for waterfall chart by inserting a NS_ESNS cookie in the response. Default value: DISABLED Possible values = ENABLED, DISABLED
webinsight	<String>	Read-write	On enabling this option, the Citrix ADC will send the webinsight records to the configured collectors. Default value: ENABLED Possible values = ENABLED, DISABLED
securityinsight	<String>	Read-write	On enabling this option, the Citrix ADC will send the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			security insight records to the configured collectors. Default value: DISABLED Possible values = ENABLED, DISABLED
botinsight	<String>	Read-write	On enabling this option, the Citrix ADC will send the bot insight records to the configured collectors. Default value: DISABLED Possible values = ENABLED, DISABLED
ciinsight	<String>	Read-write	On enabling this option, the Citrix ADC will send the ContentInspection Insight records to the configured collectors. Default value: DISABLED Possible values = ENABLED, DISABLED
videoanalytics	<String>	Read-write	On enabling this option, the Citrix ADC will send the videoinsight records

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			to the configured collectors. Default value: DISABLED Possible values = ENABLED, DISABLED
distributionalgorithm	<String>	Read-write	On enabling this option, the Citrix ADC will distribute records among the collectors. Else, all records will be sent to all the collectors. Default value: DISABLED Possible values = ENABLED, DISABLED
metricslog	<Boolean>	Read-write	If only the stats records are to be exported, turn on this option.
transactionlog	<String>	Read-write	Log ANOMALOUS or ALL transactions. Default value: ALL Possible values = ALL, ANOMALOUS
comment	<String>	Read-write	Any comments about this action. In the CLI, if including spaces between words, enclose the comment in

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			quotation marks. (The quotation marks are not required in the configuration utility.). Maximum length = 256
newname	<String>	Read-write	New name for the AppFlow action. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my appflow action" or 'my appflow action'). Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
hits	<Integer>	Read-only	The number of times the action has been taken.
referencecount	<Integer>	Read-only	The number of references to the action.
description	<String>	Read-only	Description of the action.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- RENAME
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/appflowaction **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"appflowaction":{

<b>"name":<String_value>,

</b>"collectors":<String[]_value>,

"clientsidemeasurements":<String_value>,

"pagetracking":<String_value>,

"webinsight":<String_value>,

"securityinsight":<String_value>,

"botinsight":<String_value>,
```

```
"ciinsight":<String_value>,

"videoanalytics":<String_value>,

"distributionalgorithm":<String_value>,

"metricslog":<Boolean_value>,

"transactionlog":<String_value>,

"comment":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/appflowaction/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/appflowaction **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"appflowaction":{

<b>"name":<String_value>,

</b>"collectors":<String[]_value>,

"clientsidemeasurements":<String_value>,

"comment":<String_value>,

"pagetracking":<String_value>,

"webinsight":<String_value>,

"securityinsight":<String_value>,

"botinsight":<String_value>,

"ciinsight":<String_value>,

"videoanalytics":<String_value>,

"distributionalgorithm":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/appflowaction? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"appflowaction":{

<b>"name":<String_value>,

</b>"collectors":true,

"clientsidemeasurements":true,

"comment":true,

"pagetracking":true,

"webinsight":true,

"securityinsight":true,

"botinsight":true,

"ciinsight":true,

"videoanalytics":true,

"distributionalgorithm":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

RENAME

URL: http:// <netscaler-ip-address> /nitro/v1/config/appflowaction? **action=rename HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"appflowaction":{

<b>"name":<String_value>,

</b><b>"newname":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/appflowaction **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/appflowaction? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/appflowaction? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of appflowaction resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/appflowaction? **view=summary**

Use this query-parameter to get the summary output of appflowaction resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/appflowaction? **pagesize=#no;pageno=#no**

Use this query-parameter to get the appflowaction resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "appflowaction": [ {

"name":<String_value>,

"hits":<Integer_value>,

"collectors":<String[]_value>,

"clientsidemeasurements":<String_value>,

"pagetracking":<String_value>,

"webinsight":<String_value>,

"securityinsight":<String_value>,

"botinsight":<String_value>,

"ciinsight":<String_value>,

"videoanalytics":<String_value>,

"distributionalgorithm":<String_value>,

"metricslog":<Boolean_value>,

"transactionlog":<String_value>,

"referencecount":<Integer_value>,

"description":<String_value>,
```

```
"comment":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/appflowaction/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/appflowaction/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/appflowaction/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of appflowaction resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appflowaction": [ {

"name":<String_value>,

"hits":<Integer_value>,

"collectors":<String[]_value>,

"clientsidemeasurements":<String_value>,

"pagetracking":<String_value>,

"webinsight":<String_value>,

"securityinsight":<String_value>,

"botinsight":<String_value>,

"ciinsight":<String_value>,

"videoanalytics":<String_value>,

"distributionalgorithm":<String_value>,

"metricslog":<Boolean_value>,

"transactionlog":<String_value>,

"referencecount":<Integer_value>,

"description":<String_value>,

"comment":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/appflowaction? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "appflowaction": [ { "__count": "#no"} ] }
```

appflowaction_analyticsprofile_binding

Binding object showing the analyticsprofile that can be bound to appflowaction.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
analyticsprofile	<String>	Read-write	Analytics profile to be bound to the appflow action.
name	<String>	Read-write	Name for the action. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			hyphen (-) characters.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my appflow action" or 'my appflow action').

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/appflowaction_analyticsprofile_binding

HTTP Method: PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"appflowaction_analyticsprofile_binding":{

<b>"name":<String_value>,

</b>"analyticsprofile":<String_value>

}}
```

Response:

HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/appflowaction_analyticsprofile_binding/name_value<String>

Query-parameters:

args

http:// <netscaler-ip-address> /nitro/v1/config/appflowaction_analyticsprofile_binding/ name_value<String> ? **args=analyticsprofile: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/appflowaction_analyticsprofile_binding/ name_value<String>

Query-parameters:

filter

http:// <netscaler-ip-address> /nitro/v1/config/appflowaction_analyticsprofile_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of appflowaction_analyticsprofile_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination

http:// <netscaler-ip-address> /nitro/v1/config/appflowaction_analyticsprofile_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the appflowaction_analyticsprofile_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appflowaction_analyticsprofile_binding": [ {

"analyticsprofile":<String_value>,

"name":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/appflowaction_analyticsprofile_binding

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters:

bulkbindings

http:// <netscaler-ip-address> /nitro/v1/config/appflowaction_analyticsprofile_binding?**bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appflowaction_analyticsprofile_binding": [ {

"analyticsprofile":<String_value>,

"name":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/appflowaction_analyticsprofile_binding/name_value<String> ? **count=yes**

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"appflowaction_analyticsprofile_binding": [ { "__count": "#no"} ] }
```

appflowaction_binding

Binding object which returns the resources bound to appflowaction.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the action about which to display information.
appflowaction_analyticsprofile_binding	<appflowaction_analyticsprofile_binding[]>	Read-only	analyticsprofile that can be bound to appflowaction.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/appflowaction_binding/ name_value<String>

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "appflowaction_binding": [ {

"name":<String_value>,

"appflowaction_analyticsprofile_binding":<appflowaction_analyticsprofile_b
inding[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/appflowaction_binding

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters:

bulkbindings

http:// <netscaler-ip-address> /nitro/v1/config/appflowaction_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "appflowaction_binding": [ {

"name":<String_value>,

"appflowaction_analyticsprofile_binding":<appflowaction_analyticsprofile_b
inding[]_value>

}]}
```

appflowcollector

Configuration for AppFlow collector resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the collector. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Only four collectors can be configured. The following requirement applies

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my appflow collector" or 'my appflow collector'). Minimum length = 1 Maximum length = 127
ipaddress	<String>	Read-write	IPv4 address of the collector.
port	<Integer>	Read-write	Port on which the collector listens.
netprofile	<String>	Read-write	Netprofile to associate with the collector. The IP address defined in the profile is used as the source IP address for AppFlow traffic for this collector. If you do not set this parameter, the Citrix ADC IP (NSIP) address is used as the source IP address.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum length = 128
transport	<String>	Read-write	Type of collector: either logstream or ipfix or rest. Default value: ipfix, Possible values = ipfix, logstream
newname	<String>	Read-write	New name for the collector. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at(@), equals (=), and hyphen (-) characters. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			"my appflow coll" or 'my appflow coll'). Minimum length = 1
state	<String>	Read-only	Appflow collector state. Possible values = UP, DOWN, UNKNOWN, BUSY, OUT OF SERVICE, GOING OUT OF SERVICE, DOWN WHEN GOING OUT OF SERVICE, NS_EMPTY_STR, Unknown, DISABLED
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- UPDATE
- UNSET
- DELETE
- RENAME
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/appflowcollector **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"appflowcollector":{

<b>"name":<String_value>,

</b><b>"ipaddress":<String_value>,

</b>"port":<Integer_value>,
```

```
"netprofile":<String_value>,

"transport":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/appflowcollector **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"appflowcollector":{

<b>"name":<String_value>,

</b>"ipaddress":<String_value>,

"port":<Integer_value>,

"netprofile":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/appflowcollector? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"appflowcollector":{

<b>"name":<String_value>,

</b>"ipaddress":true,

"port":true,

"netprofile":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/appflowcollector/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

RENAME

URL: http:// <netscaler-ip-address> /nitro/v1/config/appflowcollector? **action=rename HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"appflowcollector":{

<b>"name":<String_value>,

</b><b>"newname":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/appflowcollector **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/appflowcollector? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/appflowcollector? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of appflowcollector resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/appflowcollector? **view=summary**

Use this query-parameter to get the summary output of appflowcollector resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/appflowcollector? **pagesize=#no;pageno=#no**

Use this query-parameter to get the appflowcollector resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "appflowcollector": [ {

"name":<String_value>,

"ipaddress":<String_value>,

"port":<Integer_value>,

"netprofile":<String_value>,

"transport":<String_value>,

"state":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/appflowcollector/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/appflowcollector/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/appflowcollector/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of appflowcollector resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appflowcollector": [ {

"name":<String_value>,

"ipaddress":<String_value>,

"port":<Integer_value>,
```

```
"netprofile":<String_value>,

"transport":<String_value>,

"state":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/appflowcollector? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "appflowcollector": [ { "__count": "#no"} ] }
```

appflowglobal_appflowpolicy_binding

Binding object showing the appflowpolicy that can be bound to appflowglobal.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
priority	<Integer>	Read-write	Specifies the priority of the policy.
labeltype	<String>	Read-write	Type of policy label to invoke. Specify vserver for a policy label associated with a virtual server, or policylabel for a user-defined policy label. Possible values = vserver, policylabel
type	<String>	Read-write	Global bind point for which to show detailed information about the policies bound to the bind point. Possible values = REQ_OVERRIDE, REQ_DEFAULT, OVERRIDE, DEFAULT, OTHERTCP_REQ_OVERRIDE, OTHERTCP_REQ_DEFAULT, MSSQL_REQ_OVERRIDE, MSSQL_REQ_DEFAULT, MYSQL_REQ_OVERRIDE, MYSQL_REQ_DEFAULT, ICA_REQ_OVERRI

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			DE, ICA_REQ_DEFAULT, ORACLE_REQ_OVERRIDE, ORACLE_REQ_DEFAULT, HTTPQUIC_REQ_OVERRIDE, HTTPQUIC_REQ_DEFAULT
globalbindtype	<String>	Read-write	. Default value: SYSTEM_GLOBAL Possible values = SYSTEM_GLOBAL, VPN_GLOBAL, RNAT_GLOBAL, APPFW_GLOBAL, TM_GLOBAL
policyname	<String>	Read-write	Name of the AppFlow policy.
invoke	<Boolean>	Read-write	Invoke policies bound to a virtual server or a user-defined policy label. After the invoked policies are evaluated, the flow returns to the policy with the next priority.
gotopriorityexpression	<String>	Read-write	Expression specifying the priority of the next policy

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			which will get evaluated if the current policy rule evaluates to TRUE.
labelname	<String>	Read-write	Name of the label to invoke if the current policy evaluates to TRUE.
numpol	<Integer>	Read-only	The number of policies bound to the bindpoint.
flowtype	<Integer>	Read-only	Flow type of the bound AppFlow policy.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/appflowglobal_appflowpolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"appflowglobal_appflowpolicy_binding":{

<b>"policyname":<String_value>,

</b><b>"priority":<Integer_value>,

</b>"gotopriorityexpression":<String_value>,

"type":<String_value>,

"invoke":<Boolean_value>,
```

```
"labeltype":<String_value>,

"labelname":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/appflowglobal_appflowpolicy_binding **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/appflowglobal_appflowpolicy_binding? **args= policyname:<String_value>, type: <String_value> ,priority: <Integer_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/appflowglobal_appflowpolicy_binding **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/appflowglobal_appflowpolicy_binding? **args=type: <String_value>**

Use this query-parameter to get appflowglobal_appflowpolicy_binding resources based on additional properties.

filter http:// <netscaler-ip-address> /nitro/v1/config/appflowglobal_appflowpolicy_binding? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of appflowglobal_appflowpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/appflowglobal_appflowpolicy_binding? **pagesize=#no;pageno=#no**

Use this query-parameter to get the appflowglobal_appflowpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appflowglobal_appflowpolicy_binding": [ {

"priority":<Integer_value>,

"labeltype":<String_value>,

"type":<String_value>,

"globalbindtype":<String_value>,

"policyname":<String_value>,

"invoke":<Boolean_value>,

"gotopriorityexpression":<String_value>,

"labelname":<String_value>,

"numpol":<Integer_value>,
```

```
"flowtype":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/appflowglobal_appflowpolicy_binding?**count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "appflowglobal_appflowpolicy_binding": [ { "__count": "#no"} ] }
```

appflowglobal_binding

Binding object which returns the resources bound to appflowglobal.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
appflowglobal_appflowpolicy_binding	<appflowglobal_appflowpolicy_binding[]>	Read-write	appflowpolicy that can be bound to appflowglobal.

Operations

(click to see Properties)

- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/appflowglobal_binding

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "appflowglobal_binding": [ {

"appflowglobal_appflowpolicy_binding":<appflowglobal_appflowpolicy_binding
[]_value>

}]}
```

appflowparam

Configuration for AppFlow parameter resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
templaterefresh	<Integer>	Read-write	Refresh interval, in seconds, at which to export the template data. Because data transmission is in UDP, the templates must be resent at regular intervals. Default value: 600

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum value = 60 Maximum value = 3600
appnamerefresh	<Integer>	Read-write	Interval, in seconds, at which to send Appnames to the configured collectors. Appname refers to the name of an entity (virtual server, service, or service group) in the Citrix ADC. Default value: 600 Minimum value = 60 Maximum value = 3600
flowrecordinterval	<Integer>	Read-write	Interval, in seconds, at which to send flow records to the configured collectors. Default value: 60 Minimum value = 60 Maximum value = 3600
securityinsightrecordinterval	<Integer>	Read-write	Interval, in seconds, at which to send security insight flow records to the configured collectors. Default value: 600

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum value = 60 Maximum value = 3600
udppmtu	<Integer>	Read-write	MTU, in bytes, for IPFIX UDP packets. Default value: 1472 Minimum value = 128 Maximum value = 1472
httpurl	<String>	Read-write	Include the http URL that the Citrix ADC received from the client. Default value: DISABLED Possible values = ENABLED, DISABLED
aaausername	<String>	Read-write	Enable AppFlow AAA Username logging. Default value: DISABLED Possible values = ENABLED, DISABLED
httpcookie	<String>	Read-write	Include the cookie that was in the HTTP request the appliance received from the client.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: DISABLED Possible values = ENABLED, DISABLED
httpreferer	<String>	Read-write	Include the web page that was last visited by the client. Default value: DISABLED Possible values = ENABLED, DISABLED
httpmethod	<String>	Read-write	Include the method that was specified in the HTTP request that the appliance received from the client. Default value: DISABLED Possible values = ENABLED, DISABLED
httphost	<String>	Read-write	Include the host identified in the HTTP request that the appliance received from the client. Default value: DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ENABLED, DISABLED
httpuseragent	<String>	Read-write	Include the client application through which the HTTP request was received by the Citrix ADC. Default value: DISABLED Possible values = ENABLED, DISABLED
clienttrafficonly	<String>	Read-write	Generate AppFlow records for only the traffic from the client. Default value: NO Possible values = YES, NO
httpcontenttype	<String>	Read-write	Include the HTTP Content-Type header sent from the server to the client to determine the type of the content sent. Default value: DISABLED Possible values = ENABLED, DISABLED
httpauthorization	<String>	Read-write	Include the HTTP Authorization header information.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: DISABLED Possible values = ENABLED, DISABLED
httpvia	<String>	Read-write	Include the httpVia header which contains the IP address of proxy server through which the client accessed the server. Default value: DISABLED Possible values = ENABLED, DISABLED
httpxforwardedfor	<String>	Read-write	Include the httpXForwardedFor header, which contains the original IP Address of the client using a proxy server to access the server. Default value: DISABLED Possible values = ENABLED, DISABLED
httplocation	<String>	Read-write	Include the HTTP location headers returned from the HTTP responses.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: DISABLED Possible values = ENABLED, DISABLED
httpsetcookie	<String>	Read-write	Include the Set-cookie header sent from the server to the client in response to a HTTP request. Default value: DISABLED Possible values = ENABLED, DISABLED
httpsetcookie2	<String>	Read-write	Include the Set-cookie header sent from the server to the client in response to a HTTP request. Default value: DISABLED Possible values = ENABLED, DISABLED
connectionchaining	<String>	Read-write	Enable connection chaining so that the client server flows of a connection are linked. Also the connection chain ID is propagated across Citrix ADCs, so that in a multi-hop

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			environment the flows belonging to the same logical connection are linked. This id is also logged as part of appflow record. Default value: DISABLED Possible values = ENABLED, DISABLED
httpdomain	<String>	Read-write	Include the http domain request to be exported. Default value: DISABLED Possible values = ENABLED, DISABLED
skipcacheredirection httptransaction	<String>	Read-write	Skip Cache http transaction. This HTTP transaction is specific to Cache Redirection module. In Case of Cache Miss there will be another HTTP transaction initiated by the cache server. Default value: DISABLED Possible values = ENABLED, DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
identifiername	<String>	Read-write	Include the stream identifier name to be exported. Default value: DISABLED Possible values = ENABLED, DISABLED
identifiersessionname	<String>	Read-write	Include the stream identifier session name to be exported. Default value: DISABLED Possible values = ENABLED, DISABLED
observationdomainid	<Integer>	Read-write	An observation domain groups a set of Citrix ADCs based on deployment: cluster, HA etc. A unique Observation Domain ID is required to be assigned to each such group. Default value: 0 Minimum value = 1000
observationdomainname	<String>	Read-write	Name of the Observation Domain defined by the observation domain ID.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum length = 127
subscriberawareness	<String>	Read-write	Enable this option for logging end user MSISDN in L4/L7 appflow records. Default value: DISABLED Possible values = ENABLED, DISABLED
subscriberidobfuscation	<String>	Read-write	Enable this option for obfuscating MSISDN in L4/L7 appflow records. Default value: DISABLED Possible values = ENABLED, DISABLED
subscriberidobfuscationalgo	<String>	Read-write	Algorithm(MD5 or SHA256) to be used for obfuscating MSISDN. Default value: MD5 Possible values = MD5, SHA256
gxsessionreporting	<String>	Read-write	Enable this option for Gx session reporting. Default value: DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ENABLED, DISABLED
securityinsighttraffic	<String>	Read-write	Enable/disable the feature individually on appflow action. Default value: DISABLED Possible values = ENABLED, DISABLED
cacheinsight	<String>	Read-write	Flag to determine whether cache records need to be exported or not. If this flag is true and IC is enabled, cache records are exported instead of L7 HTTP records. Default value: DISABLED Possible values = ENABLED, DISABLED
videoinsight	<String>	Read-write	Enable/disable the feature individually on appflow action. Default value: DISABLED Possible values = ENABLED, DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
httpquerywithurl	<String>	Read-write	Include the HTTP query segment along with the URL that the Citrix ADC received from the client. Default value: DISABLED Possible values = ENABLED, DISABLED
urlcategory	<String>	Read-write	Include the URL category record. Default value: DISABLED Possible values = ENABLED, DISABLED
lsnlogging	<String>	Read-write	On enabling this option, the Citrix ADC will send the Large Scale Nat(LSN) records to the configured collectors. Default value: DISABLED Possible values = ENABLED, DISABLED
cqareporting	<String>	Read-write	TCP CQA reporting enable/disable knob.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: DISABLED Possible values = ENABLED, DISABLED
emailaddress	<String>	Read-write	Enable AppFlow user email-id logging. Default value: DISABLED Possible values = ENABLED, DISABLED
usagerecordinterval	<Integer>	Read-write	On enabling this option, the NGS will send bandwidth usage record to configured collectors. Default value: 0 Minimum value = 0 Maximum value = 7200
websaasappusagereporting	<String>	Read-write	On enabling this option, NGS will send data used by Web/saas app at the end of every HTTP transaction to configured collectors. Default value: DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ENABLED, DISABLED
metrics	<String>	Read-write	Enable Citrix ADC Stats to be sent to the Telemetry Agent. Default value: DISABLED Possible values = ENABLED, DISABLED
events	<String>	Read-write	Enable Events to be sent to the Telemetry Agent. Default value: DISABLED Possible values = ENABLED, DISABLED
auditlogs	<String>	Read-write	Enable Auditlogs to be sent to the Telemetry Agent. Default value: DISABLED Possible values = ENABLED, DISABLED
observationpointid	<Integer>	Read-write	An observation point ID is identifier for the NetScaler from which appflow records are being exported. By default,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			the NetScaler IP is the observation point ID. Minimum value = 1
distributedtracing	<String>	Read-write	Enable generation of the distributed tracing templates in the Appflow records. Default value: DISABLED Possible values = ENABLED, DISABLED
disttracingsamplingrate	<Integer>	Read-write	Sampling rate for Distributed Tracing. Default value: 0 Minimum value = 0 Maximum value = 100
tcpattackcounterinterval	<Integer>	Read-write	Interval, in seconds, at which to send tcp attack counters to the configured collectors. If 0 is configured, the record is not sent. Default value: 0 Minimum value = 0 Maximum value = 3600
logstreamovernsip	<String>	Read-write	To use the Citrix ADC IP to send

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Logstream records instead of the SNIP. Default value: DISABLED Possible values = ENABLED, DISABLED
analyticsauthtoken	<String>	Read-write	Authentication token to be set by the agent. Maximum length = 512
timeseriesovernsip	<String>	Read-write	To use the Citrix ADC IP to send Time series data such as metrics and events, instead of the SNIP. Default value: DISABLED Possible values = ENABLED, DISABLED
logalljsonfields	<String>	Read-write	Overrides the field filtering for all analytics profiles, and sends all the fields for the configured insights. Default value: DISABLED Possible values = ENABLED, DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
builtin	<String[]>	Read-only	Flag to determine if the appflow param is built-in or not. Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL
feature	<String>	Read-only	The feature to be checked while applying this config.
tcpburstreporting	<String>	Read-only	TCP burst reporting enable/disable knob. Default value: ENABLED Possible values = ENABLED, DISABLED
tcpburstreportingthreshold	<Integer>	Read-only	TCP burst reporting threshold. Default value: 1500 Minimum value = 10 Maximum value = 5000
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- UPDATE
- UNSET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/appflowparam **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"appflowparam":{

"templaterefresh":<Integer_value>,

"appnamerefresh":<Integer_value>,
```

```
"flowrecordinterval":<Integer_value>,

"securityinsightrecordinterval":<Integer_value>,

"udppmtu":<Integer_value>,

"httpurl":<String_value>,

"aaausername":<String_value>,

"httpcookie":<String_value>,

"httpreferer":<String_value>,

"httpmethod":<String_value>,

"httphost":<String_value>,

"httpuseragent":<String_value>,

"clienttrafficonly":<String_value>,

"httpcontenttype":<String_value>,

"httpauthorization":<String_value>,

"httpvia":<String_value>,

"httpxforwardedfor":<String_value>,

"httplocation":<String_value>,

"httpsetcookie":<String_value>,

"httpsetcookie2":<String_value>,

"connectionchaining":<String_value>,

"httpdomain":<String_value>,

"skipcacheredirectionhttptransaction":<String_value>,

"identifiername":<String_value>,
```

```
"identifiersessionname":<String_value>,

"observationdomainid":<Integer_value>,

"observationdomainname":<String_value>,

"subscriberawareness":<String_value>,

"subscriberidobfuscation":<String_value>,

"subscriberidobfuscationalgo":<String_value>,

"gxsessionreporting":<String_value>,

"securityinsighttraffic":<String_value>,

"cacheinsight":<String_value>,

"videoinsight":<String_value>,

"httpquerywithurl":<String_value>,

"urlcategory":<String_value>,

"lsnlogging":<String_value>,

"cqareporting":<String_value>,

"emailaddress":<String_value>,

"usagerecordinterval":<Integer_value>,

"websaasappusagereporting":<String_value>,

"metrics":<String_value>,

"events":<String_value>,

"auditlogs":<String_value>,

"observationpointid":<Integer_value>,

"distributedtracing":<String_value>,
```

```
"disttracingsamplingrate":<Integer_value>,

"tcpattackcounterinterval":<Integer_value>,

"logstreamovernsip":<String_value>,

"analyticsauthtoken":<String_value>,

"timeseriesovernsip":<String_value>,

"logalljsonfields":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/appflowparam? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"appflowparam":{

"templaterefresh":true,

"appnamerefresh":true,

"flowrecordinterval":true,

"securityinsightrecordinterval":true,
```

```
"udppmtu":true,

"httpurl":true,

"aaausername":true,

"httpcookie":true,

"httpreferer":true,

"httpmethod":true,

"httphost":true,

"httpuseragent":true,

"clienttrafficonly":true,

"httpcontenttype":true,

"httpauthorization":true,

"httpvia":true,

"httpxforwardedfor":true,

"httplocation":true,

"httpsetcookie":true,

"httpsetcookie2":true,

"connectionchaining":true,

"httpdomain":true,

"skipcacheredirectionhttptransaction":true,

"identifiername":true,

"identifiersessionname":true,

"observationdomainid":true,
```

```
"observationdomainname":true,

"subscriberawareness":true,

"subscriberidobfuscation":true,

"subscriberidobfuscationalgo":true,

"gxsessionreporting":true,

"securityinsighttraffic":true,

"cacheinsight":true,

"videoinsight":true,

"httpquerywithurl":true,

"urlcategory":true,

"lsnlogging":true,

"cqareporting":true,

"emailaddress":true,

"usagerecordinterval":true,

"websaasappusagereporting":true,

"metrics":true,

"events":true,

"auditlogs":true,

"observationpointid":true,

"distributedtracing":true,

"disttracingsamplingrate":true,

"tcpattackcounterinterval":true,
```

```
"logstreamovernsip":true,

"analyticsauthtoken":true,

"timeseriesovernsip":true,

"logalljsonfields":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/appflowparam **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "appflowparam": [ {

"templaterefresh":<Integer_value>,

"appnamerefresh":<Integer_value>,

"flowrecordinterval":<Integer_value>,
```

```
"securityinsightrecordinterval":<Integer_value>,

"udppmtu":<Integer_value>,

"httpurl":<String_value>,

"aaausername":<String_value>,

"httpcookie":<String_value>,

"httpreferer":<String_value>,

"httpmethod":<String_value>,

"httphost":<String_value>,

"httpuseragent":<String_value>,

"clienttrafficonly":<String_value>,

"httpcontenttype":<String_value>,

"httpauthorization":<String_value>,

"httpvia":<String_value>,

"httpxforwardedfor":<String_value>,

"httplocation":<String_value>,

"httpsetcookie":<String_value>,

"httpsetcookie2":<String_value>,

"connectionchaining":<String_value>,

"httpdomain":<String_value>,

"skipcacheredirectionhttptransaction":<String_value>,

"identifiername":<String_value>,

"identifiersessionname":<String_value>,
```

```
"observationdomainid":<Integer_value>,

"observationpointid":<Integer_value>,

"observationdomainname":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"securityinsighttraffic":<String_value>,

"subscriberawareness":<String_value>,

"subscriberidobfuscation":<String_value>,

"subscriberidobfuscationalgo":<String_value>,

"gxsessionreporting":<String_value>,

"cacheinsight":<String_value>,

"videoinsight":<String_value>,

"httpquerywithurl":<String_value>,

"tcpburstreporting":<String_value>,

"tcpburstreportingthreshold":<Integer_value>,

"urlcategory":<String_value>,

"lsnlogging":<String_value>,

"cqareporting":<String_value>,

"emailaddress":<String_value>,

"usagerecordinterval":<Integer_value>,

"websaasappusagereporting":<String_value>,

"metrics":<String_value>,
```

```
"events":<String_value>,

"auditlogs":<String_value>,

"distributedtracing":<String_value>,

"disttracingsamplingrate":<Integer_value>,

"tcpattackcounterinterval":<Integer_value>,

"logstreamovernsip":<String_value>,

"analyticsauthtoken":<String_value>,

"timeseriesovernsip":<String_value>,

"logalljsonfields":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

appflowpolicy

Configuration for AppFlow policy resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the policy. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			(@), equals (=), and hyphen (-) characters. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my appflow policy" or 'my appflow policy').
rule	<String>	Read-write	Expression or other value against which the traffic is evaluated. Must be a Boolean expression. The following requirements apply only to the Citrix ADC CLI: * If the expression includes one or more spaces, enclose the entire expression in double quotation marks.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			* If the expression itself includes double quotation marks, escape the quotations by using the \ character. * Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks.
action	<String>	Read-write	Name of the action to be associated with this policy.
undefaction	<String>	Read-write	Name of the appflow action to be associated with this policy when an undef event occurs.
comment	<String>	Read-write	Any comments about this policy.
newname	<String>	Read-write	New name for the policy. Must begin with an ASCII alphabetic or underscore (_)character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@),

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			equals (=), and hyphen (-) characters. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my appflow policy" or 'my appflow policy'). Minimum length = 1
hits	<Integer>	Read-only	Number of hits.
undefhits	<Integer>	Read-only	Number of policy UNDEF hits.
description	<String>	Read-only	Description of the policy.
builtin	<String[]>	Read-only	Flag to determine if policy is built-in or not. Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
feature	<String>	Read-only	The feature to be checked while applying this config.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- RENAME
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/appflowpolicy **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"appflowpolicy":{

<b>"name":<String_value>,

</b><b>"rule":<String_value>,

</b><b>"action":<String_value>,

</b>"undefaction":<String_value>,

"comment":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/appflowpolicy/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/appflowpolicy **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"appflowpolicy":{

<b>"name":<String_value>,

</b>"rule":<String_value>,

"action":<String_value>,

"undefaction":<String_value>,

"comment":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/appflowpolicy? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"appflowpolicy":{

<b>"name":<String_value>,

</b>"undefaction":true,

"comment":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

RENAME

URL: http:// <netscaler-ip-address> /nitro/v1/config/appflowpolicy? **action=rename HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"appflowpolicy":{

<b>"name":<String_value>,

</b><b>"newname":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/appflowpolicy **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/appflowpolicy? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/appflowpolicy? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of appflowpolicy resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/appflowpolicy? **view=summary**

Use this query-parameter to get the summary output of appflowpolicy resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/appflowpolicy? **pagesize=#no;pageno=#no**

Use this query-parameter to get the appflowpolicy resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "appflowpolicy": [ {

"name":<String_value>,

"rule":<String_value>,

"action":<String_value>,

"undefaction":<String_value>,

"hits":<Integer_value>,

"undefhits":<Integer_value>,

"description":<String_value>,

"comment":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/appflowpolicy/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/appflowpolicy/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/appflowpolicy/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of appflowpolicy resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appflowpolicy": [ {

"name":<String_value>,

"rule":<String_value>,

"action":<String_value>,

"undefaction":<String_value>,

"hits":<Integer_value>,

"undefhits":<Integer_value>,

"description":<String_value>,

"comment":<String_value>,

"builtin":<String[]_value>,
```

```
"feature":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/appflowpolicy? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "appflowpolicy": [ { "__count": "#no"} ] }
```

appflowpolicy_appflowglobal_binding

Binding object showing the appflowglobal that can be bound to appflowpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
boundto	<String>	Read-write	Location where policy is bound.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the policy about which to display detailed information.
labeltype	<String>	Read-only	Type of policy label invocation. Possible values = vserver, policylabel
priority	<Integer>	Read-only	Specifies the priority of the policy.
labelname	<String>	Read-only	Name of the label to invoke if the current policy rule evaluates to TRUE.
gotopriorityexpression	<String>	Read-only	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
activepolicy	<Integer>	Read-only	Indicates whether policy is bound or not.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/appflowpolicy_appflowglobal_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ appflowpolicy_appflowglobal_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of appflowpolicy_appflowglobal_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/appflowpolicy_appflowglobal_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the appflowpolicy_appflowglobal_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appflowpolicy_appflowglobal_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"labelname":<String_value>,

"gotopriorityexpression":<String_value>,

"activepolicy":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/appflowpolicy_appflowglobal_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/appflowpolicy_appflowglobal_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appflowpolicy_appflowglobal_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"labelname":<String_value>,

"gotopriorityexpression":<String_value>,

"activepolicy":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/appflowpolicy_appflowglobal_binding/name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"appflowpolicy_appflowglobal_binding": [ { "__count": "#no"} ] }
```

appflowpolicy_appflowpolicylabel_binding

Binding object showing the appflowpolicylabel that can be bound to appflowpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the policy about which to display detailed information.
boundto	<String>	Read-write	Location where policy is bound.
labelname	<String>	Read-only	Name of the label to invoke if the current policy rule evaluates to TRUE.
gotopriorityexpression	<String>	Read-only	Expression specifying the priority of the next policy which will get

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			evaluated if the current policy rule evaluates to TRUE.
activepolicy	<Integer>	Read-only	Indicates whether policy is bound or not.
labeltype	<String>	Read-only	Type of policy label invocation. Possible values = vserver, policylabel
priority	<Integer>	Read-only	Specifies the priority of the policy.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/appflowpolicy_appflowpolicylabel_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ appflowpolicy_appflowpolicylabel_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of appflowpolicy_appflowpolicylabel_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ appflowpolicy_appflowpolicylabel_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the appflowpolicy_appflowpolicylabel_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appflowpolicy_appflowpolicylabel_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"labelname":<String_value>,

"gotopriorityexpression":<String_value>,

"activepolicy":<Integer_value>,

"labeltype":<String_value>,

"priority":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/appflowpolicy_appflowpolicylabel_binding
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/appflowpolicy_appflowpolicylabel_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appflowpolicy_appflowpolicylabel_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"labelname":<String_value>,

"gotopriorityexpression":<String_value>,

"activepolicy":<Integer_value>,

"labeltype":<String_value>,

"priority":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/appflowpolicy_appflowpolicylabel_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"appflowpolicy_appflowpolicylabel_binding": [ { "__count": "#no"} ] }
```

appflowpolicy_binding

Binding object which returns the resources bound to appflowpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the policy about which to display detailed information.
appflowpolicy_lbvserver_binding	<appflowpolicy_lbvserver_binding[]>	Read-only	lbvserver that can be bound to appflowpolicy.
appflowpolicy_vpnvserver_binding	<appflowpolicy_vpnvserver_binding[]>	Read-only	vpnvserver that can be bound to appflowpolicy.
appflowpolicy_appflowpolicylabel_binding	<appflowpolicy_appflowpolicylabel_binding[]>	Read-only	appflowpolicylabel that can be bound to appflowpolicy.
appflowpolicy_appflowglobal_binding	<appflowpolicy_appflowglobal_binding[]>	Read-only	appflowglobal that can be bound to appflowpolicy.
appflowpolicy_csvserver_binding	<appflowpolicy_csvserver_binding[]>	Read-only	csvserver that can be bound to appflowpolicy.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/appflowpolicy_binding/ name_value<String>
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "appflowpolicy_binding": [ {

"name":<String_value>,

"appflowpolicy_csvserver_binding":<appflowpolicy_csvserver_binding[]_value
>,

"appflowpolicy_appflowpolicylabel_binding":<appflowpolicy_appflowpolicylab
el_binding[]_value>,

"appflowpolicy_appflowglobal_binding":<appflowpolicy_appflowglobal_binding
[]_value>,

"appflowpolicy_lbvserver_binding":<appflowpolicy_lbvserver_binding[]_value
>,

"appflowpolicy_vpnvserver_binding":<appflowpolicy_vpnvserver_binding[]_val
ue>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/appflowpolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/appflowpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "appflowpolicy_binding": [ {

"name":<String_value>,

"appflowpolicy_csvserver_binding":<appflowpolicy_csvserver_binding[]_value
>,

"appflowpolicy_appflowpolicylabel_binding":<appflowpolicy_appflowpolicylab
el_binding[]_value>,

"appflowpolicy_appflowglobal_binding":<appflowpolicy_appflowglobal_binding
[]_value>,

"appflowpolicy_lbvserver_binding":<appflowpolicy_lbvserver_binding[]_value
>,

"appflowpolicy_vpnvserver_binding":<appflowpolicy_vpnvserver_binding[]_val
ue>

}]}
```

appflowpolicy_csvserver_binding

Binding object showing the csvserver that can be bound to appflowpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
boundto	<String>	Read-write	Location where policy is bound.
name	<String>	Read-write	Name of the policy about which to display detailed information.
labeltype	<String>	Read-only	Type of policy label invocation. Possible values = vserver, policylabel
priority	<Integer>	Read-only	Specifies the priority of the policy.
labelname	<String>	Read-only	Name of the label to invoke if the current policy rule evaluates to TRUE.
gotopriorityexpression	<String>	Read-only	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
activepolicy	<Integer>	Read-only	Indicates whether policy is bound or not.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)

- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/appflowpolicy_csvserver_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ appflowpolicy_csvserver_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of appflowpolicy_csvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/appflowpolicy_csvserver_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the appflowpolicy_csvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appflowpolicy_csvserver_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"labelname":<String_value>,

"gotopriorityexpression":<String_value>,

"activepolicy":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/appflowpolicy_csvserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/appflowpolicy_csvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appflowpolicy_csvserver_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"labelname":<String_value>,

"gotopriorityexpression":<String_value>,

"activepolicy":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/appflowpolicy_csvserver_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"appflowpolicy_csvserver_binding": [ { "__count": "#no"} ] }
```

appflowpolicy_lbvserver_binding

Binding object showing the lbvserver that can be bound to appflowpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the policy about which to display detailed information.
boundto	<String>	Read-write	Location where policy is bound.
labelname	<String>	Read-only	Name of the label to invoke if the current

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			policy rule evaluates to TRUE.
gotopriorityexpression	<String>	Read-only	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
activepolicy	<Integer>	Read-only	Indicates whether policy is bound or not.
labeltype	<String>	Read-only	Type of policy label invocation. Possible values = vserver, policylabel
priority	<Integer>	Read-only	Specifies the priority of the policy.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/appflowpolicy_lbvserver_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ appflowpolicy_lbvserver_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of appflowpolicy_lbvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/appflowpolicy_lbvserver_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the appflowpolicy_lbvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appflowpolicy_lbvserver_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"labelname":<String_value>,

"gotopriorityexpression":<String_value>,

"activepolicy":<Integer_value>,

"labeltype":<String_value>,

"priority":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/appflowpolicy_lbvserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/appflowpolicy_lbvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appflowpolicy_lbvserver_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"labelname":<String_value>,

"gotopriorityexpression":<String_value>,

"activepolicy":<Integer_value>,

"labeltype":<String_value>,

"priority":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/appflowpolicy_lbvserver_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"appflowpolicy_lbvserver_binding": [ { "__count": "#no"} ] }
```

appflowpolicy_vpnvserver_binding

Binding object showing the vpnvserver that can be bound to appflowpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
boundto	<String>	Read-write	Location where policy is bound.
name	<String>	Read-write	Name of the policy about which to display detailed information.
labelname	<String>	Read-only	Name of the label to invoke if the current policy rule evaluates to TRUE.
gotopriorityexpression	<String>	Read-only	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
activepolicy	<Integer>	Read-only	Indicates whether policy is bound or not.
labeltype	<String>	Read-only	Type of policy label invocation. Possible values = vserver, policylabel
priority	<Integer>	Read-only	Specifies the priority of the policy.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/appflowpolicy_vpnvserver_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ appflowpolicy_vpnvserver_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of appflowpolicy_vpnvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/appflowpolicy_vpnvserver_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the appflowpolicy_vpnvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appflowpolicy_vpnvserver_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"labelname":<String_value>,

"gotopriorityexpression":<String_value>,

"activepolicy":<Integer_value>,

"labeltype":<String_value>,

"priority":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/appflowpolicy_vpnvserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/appflowpolicy_vpnvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appflowpolicy_vpnvserver_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"labelname":<String_value>,

"gotopriorityexpression":<String_value>,

"activepolicy":<Integer_value>,

"labeltype":<String_value>,

"priority":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/appflowpolicy_vpnvserver_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"appflowpolicy_vpnvserver_binding": [ { "__count": "#no"} ] }
```

appflowpolicylabel

Configuration for AppFlow policy label resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
labelname	<String>	Read-write	Name of the AppFlow policy label. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my appflow policylabel" or 'my

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			appflow policylabel'). Minimum length = 1
policylabeltype	<String>	Read-write	Type of traffic evaluated by the policies bound to the policy label. Default value: HTTP Possible values = HTTP, OTHERTCP, HTTP_QUIC
newname	<String>	Read-write	New name for the policy label. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			"my appflow policylabel" or 'my appflow policylabel'). Minimum length = 1
numpol	<Integer>	Read-only	Number of polices bound to the policy label.
hits	<Integer>	Read-only	Number of times the policy label was invoked.
policyname	<String>	Read-only	Name of the AppFlow policy.
priority	<Integer>	Read-only	Specifies the priority of the policy.
gotopriorityexpression	<String>	Read-only	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
labeltype	<String>	Read-only	Type of policy label to be invoked. Possible values = vserver, policylabel
invoke_labelname	<String>	Read-only	Name of the label to invoke if the current policy evaluates to TRUE.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
flowtype	<Integer>	Read-only	Flowtype of the bound AppFlow policy.
description	<String>	Read-only	Description of the policylabel.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- RENAME
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/appflowpolicylabel **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"appflowpolicylabel":{

<b>"labelname":<String_value>,

</b>"policylabeltype":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/appflowpolicylabel/ labelname_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

RENAME

URL: http:// <netscaler-ip-address> /nitro/v1/config/appflowpolicylabel? **action=rename HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"appflowpolicylabel":{

<b>"labelname":<String_value>,

</b><b>"newname":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/appflowpolicylabel **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/appflowpolicylabel? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/appflowpolicylabel? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of appflowpolicylabel resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/appflowpolicylabel? **view=summary**

Use this query-parameter to get the summary output of appflowpolicylabel resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/appflowpolicylabel? **pagesize=#no;pageno=#no**

Use this query-parameter to get the appflowpolicylabel resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "appflowpolicylabel": [ {

"labelname":<String_value>,

"policylabeltype":<String_value>,

"numpol":<Integer_value>,

"hits":<Integer_value>,

"policyname":<String_value>,

"priority":<Integer_value>,

"gotopriorityexpression":<String_value>,
```

```
"labeltype":<String_value>,

"invoke_labelname":<String_value>,

"flowtype":<Integer_value>,

"description":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/appflowpolicylabel/ labelname_value<String>
Query-parameters: attrs http:// <netscaler-ip-address> /nitro/v1/config/appflowpolicylabel/ labelname_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/appflowpolicylabel/ labelname_value<String> ? **view=summary**

Use this query-parameter to get the summary output of appflowpolicylabel resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appflowpolicylabel": [ {

"labelname":<String_value>,

"policylabeltype":<String_value>,

"numpol":<Integer_value>,

"hits":<Integer_value>,

"policyname":<String_value>,

"priority":<Integer_value>,

"gotopriorityexpression":<String_value>,

"labeltype":<String_value>,

"invoke_labelname":<String_value>,

"flowtype":<Integer_value>,

"description":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/appflowpolicylabel? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "appflowpolicylabel": [ { "__count": "#no"} ] }
```

appflowpolicylabel_appflowpolicy_binding

Binding object showing the appflowpolicy that can be bound to appflowpolicylabel.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
labeltype	<String>	Read-write	Type of policy label to be invoked. Possible values = vserver, policylabel
priority	<Integer>	Read-write	Specifies the priority of the policy.
policyname	<String>	Read-write	Name of the AppFlow policy.
invoke_labelname	<String>	Read-write	Name of the label to invoke if the current policy evaluates to TRUE.
labelname	<String>	Read-write	Name of the policy label to which to bind the policy.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum length = 1
gotopriorityexpression	<String>	Read-write	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
invoke	<Boolean>	Read-write	Invoke policies bound to a virtual server or a user-defined policy label. After the invoked policies are evaluated, the flow returns to the policy with the next priority.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/appflowpolicylabel_appflowpolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"appflowpolicylabel_appflowpolicy_binding":{

<b>"labelname":<String_value>,

</b><b>"policyname":<String_value>,

</b><b>"priority":<Integer_value>,

</b>"gotopriorityexpression":<String_value>,
```

```
"invoke":<Boolean_value>,

"labeltype":<String_value>,

"invoke_labelname":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/appflowpolicylabel_appflowpolicy_binding/ labelname_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ appflowpolicylabel_appflowpolicy_binding/ labelname_value<String> ? **args= policyname:<String_value>, priority: <Integer_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/appflowpolicylabel_appflowpolicy_binding/ labelname_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ appflowpolicylabel_appflowpolicy_binding/ labelname_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of appflowpolicylabel_appflowpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ appflowpolicylabel_appflowpolicy_binding/ labelname_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the appflowpolicylabel_appflowpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appflowpolicylabel_appflowpolicy_binding": [ {

"labeltype":<String_value>,

"priority":<Integer_value>,

"policyname":<String_value>,

"invoke_labelname":<String_value>,

"labelname":<String_value>,

"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/appflowpolicylabel_appflowpolicy_binding
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/appflowpolicylabel_appflowpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appflowpolicylabel_appflowpolicy_binding": [ {

"labeltype":<String_value>,

"priority":<Integer_value>,

"policyname":<String_value>,

"invoke_labelname":<String_value>,

"labelname":<String_value>,

"gotopriorityexpression":<String_value>,
```

```
"invoke":<Boolean_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/appflowpolicylabel_appflowpolicy_binding/ labelname_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"appflowpolicylabel_appflowpolicy_binding": [ { "__count": "#no"} ] }
```

appflowpolicylabel_binding

Binding object which returns the resources bound to appflowpolicylabel.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
labelname	<String>	Read-write	Name of the policy label about which to display detailed information.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum length = 1
appflowpolicylabel_appflowpolicy_binding	<appflowpolicylabel_appflowpolicy_binding[]>	Read-only	appflowpolicy that can be bound to appflowpolicylabel.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/appflowpolicylabel_binding/ labelname_value<String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "appflowpolicylabel_binding": [ {

"labelname":<String_value>,

"appflowpolicylabel_appflowpolicy_binding":<appflowpolicylabel_appflowpoli
cy_binding[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/appflowpolicylabel_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ appflowpolicylabel_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "appflowpolicylabel_binding": [ {

"labelname":<String_value>,

"appflowpolicylabel_appflowpolicy_binding":<appflowpolicylabel_appflowpoli
cy_binding[]_value>

}]}
```

appfw

Application Firewall

Application Firewall configuration.

NAME	DESCRIPTION
appfwarchive	Configuration for archive
appfwconfidfield	Configuration for configured confidential form fields
appfwcustomsettings	Configuration for application firewall custom settings XML configuration

NAME	DESCRIPTION
appfwfieldtype	Configuration for application firewall form field type
appfwglobal_appfwpolicy_binding	Binding object showing the appfwpolicy that can be bound to appfwglobal
appfwglobal_auditnslogpolicy_binding	Binding object showing the auditnslogpolicy that can be bound to appfwglobal
appfwglobal_auditsyslogpolicy_binding	Binding object showing the auditsyslogpolicy that can be bound to appfwglobal
appfwglobal_binding	Binding object showing the resources that can be bound to appfwglobal
appfwgrpccontenttype	Configuration for gRRPC content type
appfwgrpcwebjsoncontenttype	Configuration for gRRPC-Web-json content type
appfwgrpcwebtextcontenttype	Configuration for gRRPC-Web-text content type
appfwhtmlerrorpage	Configuration for HTML error page
appfwjsoncontenttype	Configuration for JSON content type
appfwjsonerrorpage	Configuration for JSON error page
appfwlearningdata	Configuration for learning data

NAME	DESCRIPTION
appfwlearningsettings	Configuration for learning settings
appfwmultipartformcontenttype	Configuration for Multipart form content type
appfwpolicy	Configuration for application firewall policy
appfwpolicy_appfwglobal_binding	Binding object showing the appfwglobal that can be bound to appfwpolicy
appfwpolicy_appfwpolicylabel_binding	Binding object showing the appfwpolicylabel that can be bound to appfwpolicy
appfwpolicy_binding	Binding object showing the resources that can be bound to appfwpolicy
appfwpolicy_csvserver_binding	Binding object showing the csvserver that can be bound to appfwpolicy
appfwpolicy_lbvserver_binding	Binding object showing the lbvserver that can be bound to appfwpolicy
appfwpolicy_vpnvserver_binding	Binding object showing the vpnvserver that can be bound to appfwpolicy
appfwpolicylabel	Configuration for application firewall policy label
appfwpolicylabel_appfwpolicy_binding	Binding object showing the appfwpolicy that can be bound to appfwpolicylabel

NAME	DESCRIPTION
appfwpolicylabel_binding	Binding object showing the resources that can be bound to appfwpolicylabel
appfwpolicylabel_policybinding_binding	Binding object showing the policybinding that can be bound to appfwpolicylabel
appfwprofile	Configuration for application firewall profile
appfwprofile_appfwconfidfield_binding	Binding object showing the appfwconfidfield that can be bound to appfwprofile
appfwprofile_binding	Binding object showing the resources that can be bound to appfwprofile
appfwprofile_blockkeyword_binding	Binding object showing the blockkeyword that can be bound to appfwprofile
appfwprofile_bypasslist_binding	Binding object showing the bypasslist that can be bound to appfwprofile
appfwprofile_cmdinjection_binding	Binding object showing the cmdinjection that can be bound to appfwprofile
appfwprofile_contenttype_binding	Binding object showing the contenttype that can be bound to appfwprofile
appfwprofile_cookieconsistency_binding	Binding object showing the cookieconsistency that can be bound to appfwprofile

NAME	DESCRIPTION
appfwprofile_creditcardnumber_binding	Binding object showing the creditcardnumber that can be bound to appfwprofile
appfwprofile_crosssitescripting_binding	Binding object showing the crosssitescripting that can be bound to appfwprofile
appfwprofile_csrftag_binding	Binding object showing the csrftag that can be bound to appfwprofile
appfwprofile_denylist_binding	Binding object showing the denylist that can be bound to appfwprofile
appfwprofile_denyurl_binding	Binding object showing the denyurl that can be bound to appfwprofile
appfwprofile_excluderescontenttype_binding	Binding object showing the excluderescontenttype that can be bound to appfwprofile
appfwprofile_fakeaccount_binding	Binding object showing the fakeaccount that can be bound to appfwprofile
appfwprofile_fieldconsistency_binding	Binding object showing the fieldconsistency that can be bound to appfwprofile
appfwprofile_fieldformat_binding	Binding object showing the fieldformat that can be bound to appfwprofile
appfwprofile_fileuploadtype_binding	Binding object showing the fileuploadtype that can be bound to appfwprofile

NAME	DESCRIPTION
appfwprofile_grpcvalidation_binding	Binding object showing the grpcvalidation that can be bound to appfwprofile
appfwprofile_jsonblockkeyword_binding	Binding object showing the jsonblockkeyword that can be bound to appfwprofile
appfwprofile_jsoncmdurl_binding	Binding object showing the jsoncmdurl that can be bound to appfwprofile
appfwprofile_jsondosurl_binding	Binding object showing the jsondosurl that can be bound to appfwprofile
appfwprofile_jsonsqlurl_binding	Binding object showing the jsonsqlurl that can be bound to appfwprofile
appfwprofile_jsonxssurl_binding	Binding object showing the jsonxssurl that can be bound to appfwprofile
appfwprofile_logexpression_binding	Binding object showing the logexpression that can be bound to appfwprofile
appfwprofile_restvalidation_binding	Binding object showing the restvalidation that can be bound to appfwprofile
appfwprofile_safeobject_binding	Binding object showing the safeobject that can be bound to appfwprofile
appfwprofile_sqlinjection_binding	Binding object showing the sqlinjection that can be bound to appfwprofile

NAME	DESCRIPTION
appfwprofile_starturl_binding	Binding object showing the starturl that can be bound to appfwprofile
appfwprofile_trustedlearningclients_binding	Binding object showing the trustedlearningclients that can be bound to appfwprofile
appfwprofile_xmlattachmenturl_binding	Binding object showing the xmlattachmenturl that can be bound to appfwprofile
appfwprofile_xmldosurl_binding	Binding object showing the xmldosurl that can be bound to appfwprofile
appfwprofile_xmlsqlinjection_binding	Binding object showing the xmlsqlinjection that can be bound to appfwprofile
appfwprofile_xmlvalidationurl_binding	Binding object showing the xmlvalidationurl that can be bound to appfwprofile
appfwprofile_xmlwsiurl_binding	Binding object showing the xmlwsiurl that can be bound to appfwprofile
appfwprofile_xmlxss_binding	Binding object showing the xmlxss that can be bound to appfwprofile
appfwprotofile	Configuration for gRPC protofile
appfwsettings	Configuration for AS settings
appfwsignatures	Configuration for application firewall signatures XML configuration

NAME	DESCRIPTION
appfwtransactionrecords	Configuration for Application firewall transaction record
appfwurlencodedformcontenttype	Configuration for Urlencoded form content type
appfwwsdl	Configuration for WSDL file
appfwxmlcontenttype	Configuration for XML Content type
appfwxmlerrorpage	Configuration for xml error page
appfwxmlschema	Configuration for XML schema

appfwarchive

Configuration for archive resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of tar archive. Minimum length = 1
target	<String>	Read-write	Path to the file to be exported. Minimum length = 1 Maximum length = 2047

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
src	<String>	Read-write	Indicates the source of the tar archive file as a URL of the form <protocol>://<host>[:<port>][/<path>] <protocol> is http or https. <host> is the DNS name or IP address of the http or https server. <port> is the port number of the server. If omitted, the default port for http or https will be used. <path> is the path of the file on the server. Import will fail if an https server requires client certificate authentication. .

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum length = 1 Maximum length = 2047
comment	<String>	Read-write	Comments associated with this archive. Maximum length = 128
response	<String>	Read-only	.
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- GET (ALL)
- EXPORT
- IMPORT
- DELETE

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.
- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

EXPORT

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwarchive? **action=export HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"appfwarchive":{

<b>"name":<String_value>,

</b><b>"target":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

IMPORT

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwarchive? **action=Import HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"appfwarchive":{

<b>"src":<String_value>,

</b><b>"name":<String_value>,

</b>"comment":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwarchive/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwarchive **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "appfwarchive": [ {

"response":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

appfwconfidfield

Configuration for configured confidential form fields resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
fieldname	<String>	Read-write	Name of the form field to designate as confidential. Minimum length = 1
url	<String>	Read-write	URL of the web page that contains the web form. Minimum length = 1
isregex	<String>	Read-write	Method of specifying the form field name.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Available settings function as follows: * REGEX. Form field is a regular expression. * NOTREGEX. Form field is a literal string. Default value: NOTREGEX Possible values = REGEX, NOTREGEX
comment	<String>	Read-write	Any comments to preserve information about the form field designation.
state	<String>	Read-write	Enable or disable the confidential field designation. Default value: ENABLED Possible values = ENABLED, DISABLED
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD

- DELETE
- UPDATE
- UNSET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwconfidfield **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"appfwconfidfield":{

<b>"fieldname":<String_value>,

</b><b>"url":<String_value>,

</b>"isregex":<String_value>,

"comment":<String_value>,

"state":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwconfidfield/ fieldname_value<String>
Query-parameters: args= url:<String_value>

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwconfidfield **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"appfwconfidfield":{

<b>"fieldname":<String_value>,

</b><b>"url":<String_value>,

</b>"comment":<String_value>,

"isregex":<String_value>,

"state":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwconfidfield? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"appfwconfidfield":{

<b>"fieldname":<String_value>,

</b><b>"url":<String_value>,

</b>"comment":true,
```

```
"isregex":true,

"state":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwconfidfield **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/appfwconfidfield? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/appfwconfidfield? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of appfwconfidfield resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/appfwconfidfield? **view=summary**

Use this query-parameter to get the summary output of appfwconfidfield resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/appfwconfidfield? **pagesize=#no;pageno=#no**

Use this query-parameter to get the appfwconfidfield resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "appfwconfidfield": [ {

"fieldname":<String_value>,

"url":<String_value>,

"isregex":<String_value>,

"comment":<String_value>,

"state":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwconfidfield? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "appfwconfidfield": [ { "__count": "#no"} ] }
```

appfwcustomsettings

Configuration for application firewall custom settings XML configuration resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	. Minimum length = 1
target	<String>	Read-write	. Minimum length = 1 Maximum length = 2047

Operations

(click to see Properties)

- EXPORT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

EXPORT

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwcustomsettings? **action=export HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"appfwcustomsettings":{

<b>"name":<String_value>,

</b><b>"target":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

appfwfieldtype

Configuration for application firewall form field type resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the field type. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after the field type is added. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			"my field type" or 'my field type'). Minimum length = 1
regex	<String>	Read-write	PCRE - format regular expression defining the characters and length allowed for this field type. Minimum length = 1
priority	<Integer>	Read-write	Positive integer specifying the priority of the field type. A lower number specifies a higher priority. Field types are checked in the order of their priority numbers. Minimum value = 0 Maximum value = 64000
comment	<String>	Read-write	Comment describing the type of field that this field type is intended to match.
nocharmaps	<Boolean>	Read-write	will not show internal field types added as part of FieldFormat learn rules deployment.
builtin	<String[]>	Read-only	Flag to determine if fieldtype is built-in or not.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL
feature	<String>	Read-only	The feature to be checked while applying this config.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of

creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwfieldtype **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"appfwfieldtype":{

<b>"name":<String_value>,

</b><b>"regex":<String_value>,

</b><b>"priority":<Integer_value>,

</b>"comment":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwfieldtype/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwfieldtype **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"appfwfieldtype":{

<b>"name":<String_value>,

</b><b>"regex":<String_value>,

</b><b>"priority":<Integer_value>,

</b>"comment":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwfieldtype **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/appfwfieldtype? **args=name: <String_value> ,nocharmaps: <Boolean_value>**

Use this query-parameter to get appfwfieldtype resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/config/appfwfieldtype? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/appfwfieldtype? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of appfwfieldtype resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/appfwfieldtype? **view=summary**

Use this query-parameter to get the summary output of appfwfieldtype resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/appfwfieldtype? **pagesize=#no;pageno=#no**

Use this query-parameter to get the appfwfieldtype resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "appfwfieldtype": [ {

name:<String_value>,nocharmaps:<Boolean_value>"regex":<String_value>,

"priority":<Integer_value>,

"comment":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwfieldtype/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/appfwfieldtype/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/appfwfieldtype/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of appfwfieldtype resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwfieldtype": [ {

name:<String_value>,nocharmaps:<Boolean_value>"regex":<String_value>,

"priority":<Integer_value>,

"comment":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwfieldtype? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "appfwfieldtype": [ { "__count": "#no"} ] }
```

appfwglobal_appfwpolicy_binding

Binding object showing the appfwpolicy that can be bound to appfwglobal.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
policyname	<String>	Read-write	Name of the policy.
priority	<Integer>	Read-write	The priority of the policy.
globalbindtype	<String>	Read-write	. Default value: SYSTEM_GLOBAL Possible values = SYSTEM_GLOBAL, VPN_GLOBAL, RNAT_GLOBAL, APPFW_GLOBAL, TM_GLOBAL
labeltype	<String>	Read-write	Type of policy label invocation. Possible values = reqvserver, policylabel
type	<String>	Read-write	Bind point to which to policy is bound.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = REQ_OVERRIDE, REQ_DEFAULT, HTTPQUIC_REQ_OVERRIDE, HTTPQUIC_REQ_DEFAULT
state	<String>	Read-write	Enable or disable the binding to activate or deactivate the policy. This is applicable to classic policies only. Possible values = ENABLED, DISABLED
invoke	<Boolean>	Read-write	If the current policy evaluates to TRUE, terminate evaluation of policies bound to the current policy label, and then forward the request to the specified virtual server or evaluate the specified policy label.
gotopriorityexpression	<String>	Read-write	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
labelname	<String>	Read-write	Name of the policy label to invoke if the current policy

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			evaluates to TRUE, the invoke parameter is set, and Label Type is set to Policy Label.
numpol	<Integer>	Read-only	The number of policies bound to the bindpoint.
policytype	<String>	Read-only	. Possible values = Classic Policy, Advanced Policy
flowtype	<Integer>	Read-only	flowtype of the bound application firewall policy.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/appfwglobal_appfwpolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"appfwglobal_appfwpolicy_binding":{

<b>"policyname":<String_value>,

</b><b>"priority":<Integer_value>,

</b>"state":<String_value>,

"gotopriorityexpression":<String_value>,

"type":<String_value>,
```

```
"invoke":<Boolean_value>,

"labeltype":<String_value>,

"labelname":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwglobal_appfwpolicy_binding **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/appfwglobal_appfwpolicy_binding? **args= policyname:<String_value>, type: <String_value> ,priority: <Integer_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwglobal_appfwpolicy_binding **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/appfwglobal_appfwpolicy_binding? **args=type: <String_value>**

Use this query-parameter to get appfwglobal_appfwpolicy_binding resources based on additional properties.

filter http:// <netscaler-ip-address> /nitro/v1/config/appfwglobal_appfwpolicy_binding? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of appfwglobal_appfwpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/appfwglobal_appfwpolicy_binding? **pagesize=#no;pageno=#no**

Use this query-parameter to get the appfwglobal_appfwpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwglobal_appfwpolicy_binding": [ {

"policyname":<String_value>,

"priority":<Integer_value>,

"globalbindtype":<String_value>,

"labeltype":<String_value>,

"type":<String_value>,

"state":<String_value>,

"invoke":<Boolean_value>,

"gotopriorityexpression":<String_value>,
```

```
"labelname":<String_value>,

"numpol":<Integer_value>,

"policytype":<String_value>,

"flowtype":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwglobal_appfwpolicy_binding? **count=yes**
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "appfwglobal_appfwpolicy_binding": [ { "__count": "#no"} ] }
```

appfwglobal_auditnslogpolicy_binding

Binding object showing the auditnslogpolicy that can be bound to appfwglobal.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
invoke	<Boolean>	Read-write	If the current policy evaluates to TRUE, terminate evaluation of policies bound to the current policy label, and then forward the request to the specified virtual server or evaluate the specified policy label.
state	<String>	Read-write	Enable or disable the binding to activate or deactivate the policy. This is applicable to classic policies only. Possible values = ENABLED, DISABLED
gotopriorityexpression	<String>	Read-write	Expression or other value specifying the next policy to evaluate if the current policy evaluates to TRUE. Specify one of the following values: * NEXT - Evaluate the policy with the next higher priority number. * END - End policy evaluation. * USE_INVOCATION_RESULT - Applicable if this policy invokes another policy label. If the final goto in the invoked policy label

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			has a value of END, the evaluation stops. If the final goto is anything other than END, the current policy label performs a NEXT. * An expression that evaluates to a number. If you specify an expression, the number to which it evaluates determines the next policy to evaluate, as follows: * If the expression evaluates to a higher numbered priority, the policy with that priority is evaluated next. * If the expression evaluates to the priority of the current policy, the policy with the next higher numbered priority is evaluated next. * If the expression evaluates to a number that is larger than the largest numbered priority, policy evaluation ends.

An UNDEF event is triggered if:

- The expression is invalid.

- The expression evaluates to a priority number that is smaller than the current policy's priority number.
- The expression evaluates to a priority number that is between the current policy's priority number (say, 30) and the highest priority number (say, 100), but does not match any configured priority number (for example, the expression evaluates to the number 85). This example assumes that the priority number increments by 10 for every successive policy, and therefore a priority number of 85 does not exist in the policy label.
- reqvserver. Invoke the unnamed policy label associated with the specified request virtual server.
- policylabel. Invoke the specified user-defined policy label.

  Possible values = reqvserver, policylabel

  Possible values = REQ_OVERRIDE, REQ_DEFAULT, HTTPQUIC_REQ_OVERRIDE, HTTPQUIC_REQ_DEFAULT

  Possible values = Classic Policy, Advanced Policy

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.
- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of

creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/appfwglobal_auditnslogpolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"appfwglobal_auditnslogpolicy_binding":{

<b>"policyname":<String_value>,

</b><b>"priority":<Integer_value>,

</b>"state":<String_value>,

"gotopriorityexpression":<String_value>,

"type":<String_value>,

"invoke":<Boolean_value>,
```

```
"labeltype":<String_value>,

"labelname":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwglobal_auditnslogpolicy_binding **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/appfwglobal_auditnslogpolicy_binding? **args= policyname:<String_value>, type: <String_value> ,priority: <Integer_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwglobal_auditnslogpolicy_binding **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/appfwglobal_auditnslogpolicy_binding? **args=type: <String_value>**

Use this query-parameter to get appfwglobal_auditnslogpolicy_binding resources based on additional properties.

filter http:// <netscaler-ip-address> /nitro/v1/config/appfwglobal_auditnslogpolicy_binding? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of appfwglobal_auditnslogpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/appfwglobal_auditnslogpolicy_binding? **pagesize=#no;pageno=#no**

Use this query-parameter to get the appfwglobal_auditnslogpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwglobal_auditnslogpolicy_binding": [ {

"invoke":<Boolean_value>,

"state":<String_value>,

"gotopriorityexpression":<String_value>,

"labelname":<String_value>,

"priority":<Integer_value>,

"labeltype":<String_value>,

"type":<String_value>,

"policyname":<String_value>,

"policytype":<String_value>
```

```
}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwglobal_auditnslogpolicy_binding?**count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "appfwglobal_auditnslogpolicy_binding": [ { "__count": "#no"} ] }
```

appfwglobal_auditsyslogpolicy_binding

Binding object showing the auditsyslogpolicy that can be bound to appfwglobal.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
labelname	<String>	Read-write	Name of the policy label to invoke if the current policy evaluates to TRUE, the invoke parameter is set, and Label

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Type is set to Policy Label.
gotopriorityexpression	<String>	Read-write	Expression or other value specifying the next policy to evaluate if the current policy evaluates to TRUE. Specify one of the following values: * NEXT - Evaluate the policy with the next higher priority number. * END - End policy evaluation. * USE_INVOCATION_RESULT - Applicable if this policy invokes another policy label. If the final goto in the invoked policy label has a value of END, the evaluation stops. If the final goto is anything other than END, the current policy label performs a NEXT. * An expression that evaluates to a number. If you specify an expression, the number to which it evaluates determines the next policy to evaluate, as follows: * If the expression evaluates to a higher

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			numbered priority, the policy with that priority is evaluated next. * If the expression evaluates to the priority of the current policy, the policy with the next higher numbered priority is evaluated next. * If the expression evaluates to a number that is larger than the largest numbered priority, policy evaluation ends.

An UNDEF event is triggered if:

- The expression is invalid.
- The expression evaluates to a priority number that is smaller than the current policy's priority number.
- The expression evaluates to a priority number that is between the current policy's priority number (say, 30) and the highest priority number (say, 100), but does not match any configured priority number (for example, the expression evaluates to the number 85). This example assumes that the priority number increments by 10 for every successive policy, and therefore a priority number of 85 does not exist in the policy label.

  Possible values = ENABLED, DISABLED

  Possible values = REQ_OVERRIDE, REQ_DEFAULT, HTTPQUIC_REQ_OVERRIDE, HTTPQUIC_REQ_DEFAULT
- reqvserver. Invoke the unnamed policy label associated with the specified request virtual server.
- policylabel. Invoke the specified user-defined policy label.

  Possible values = reqvserver, policylabel

Possible values = Classic Policy, Advanced Policy

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/appfwglobal_auditsyslogpolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"appfwglobal_auditsyslogpolicy_binding":{

<b>"policyname":<String_value>,

</b><b>"priority":<Integer_value>,

</b>"state":<String_value>,

"gotopriorityexpression":<String_value>,

"type":<String_value>,

"invoke":<Boolean_value>,

"labeltype":<String_value>,

"labelname":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwglobal_auditsyslogpolicy_binding **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/appfwglobal_auditsyslogpolicy_binding? **args= policyname:<String_value>, type: <String_value> ,priority: <Integer_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwglobal_auditsyslogpolicy_binding **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/appfwglobal_auditsyslogpolicy_binding? **args=type: <String_value>**

Use this query-parameter to get appfwglobal_auditsyslogpolicy_binding resources based on additional properties.

filter http:// <netscaler-ip-address> /nitro/v1/config/appfwglobal_auditsyslogpolicy_binding? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of appfwglobal_auditsyslogpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/appfwglobal_auditsyslogpolicy_binding? **pagesize=#no;pageno=#no**

Use this query-parameter to get the appfwglobal_auditsyslogpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwglobal_auditsyslogpolicy_binding": [ {

"labelname":<String_value>,

"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>,

"state":<String_value>,

"type":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"policyname":<String_value>,

"policytype":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwglobal_auditsyslogpolicy_binding?**count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "appfwglobal_auditsyslogpolicy_binding": [ { "__count": "#no"} ] }
```

appfwglobal_binding

Binding object which returns the resources bound to appfwglobal.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
appfwglobal_auditnslogpolicy_binding	<appfwglobal_auditnslogpolicy_binding[]>	Read-write	auditnslogpolicy that can be bound to appfwglobal.
appfwglobal_appfwpolicy_binding	<appfwglobal_appfwpolicy_binding[]>	Read-write	appfwpolicy that can be bound to appfwglobal.
appfwglobal_auditsyslogpolicy_binding	<appfwglobal_auditsyslogpolicy_binding[]>	Read-write	auditsyslogpolicy that can be bound to appfwglobal.

Operations

(click to see Properties)

- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwglobal_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "appfwglobal_binding": [ {

"appfwglobal_auditnslogpolicy_binding":<appfwglobal_auditnslogpolicy_binding[]_value>,

"appfwglobal_appfwpolicy_binding":<appfwglobal_appfwpolicy_binding[]_value>,
```

```
"appfwglobal_auditsyslogpolicy_binding":<appfwglobal_auditsyslogpolicy_binding[]_value>

}]}
```

appfwgrpccontenttype

Configuration for gRRPC content type resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
grpccontenttypevalue	<String>	Read-write	Content type to be classified as gRPC. Minimum length = 1
isregex	<String>	Read-write	Is gRPC content type a regular expression?. Default value: NOTREGEX Possible values = REGEX, NOTREGEX
builtin	<String[]>	Read-only	Flag to determine if gRPC content type is built-in or not. Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
feature	<String>	Read-only	The feature to be checked while applying this config.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwgrpccontenttype **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"appfwgrpccontenttype":{

<b>"grpccontenttypevalue":<String_value>,

</b>"isregex":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwgrpccontenttype/ grpccontenttypevalue_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwgrpccontenttype **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/appfwgrpccontenttype? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/appfwgrpccontenttype? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of appfwgrpccontenttype resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/appfwgrpccontenttype? **view=summary**

Use this query-parameter to get the summary output of appfwgrpccontenttype resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/appfwgrpccontenttype? **pagesize=#no;pageno=#no**

Use this query-parameter to get the appfwgrpccontenttype resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "appfwgrpccontenttype": [ {

"grpccontenttypevalue":<String_value>,

"isregex":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwgrpccontenttype/ grpccontenttypevalue_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> / nitro/v1/config/appfwgrpccontenttype/ grpccontenttypevalue_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/appfwgrpccontenttype/ grpccontenttypevalue_value<String> ? **view=summary**

Use this query-parameter to get the summary output of appfwgrpccontenttype resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwgrpccontenttype": [ {

"grpccontenttypevalue":<String_value>,

"isregex":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwgrpccontenttype? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "appfwgrpccontenttype": [ { "__count": "#no"} ] }
```

appfwgrpcwebjsoncontenttype

Configuration for gRRPC-Web-json content type resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
grpcwebjsoncontenttypevalue	<String>	Read-write	Content type to be classified as gRPC-web-json. Minimum length = 1
isregex	<String>	Read-write	Is gRPC-web-json content type a regular expression?. Default value: NOTREGEX Possible values = REGEX, NOTREGEX
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwgrpcwebjsoncontenttype **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"appfwgrpcwebjsoncontenttype":{

<b>"grpcwebjsoncontenttypevalue":<String_value>,
```

```
</b>"isregex":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwgrpcwebjsoncontenttype/ grpcwebjsoncontenttypevalue_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwgrpcwebjsoncontenttype **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/appfwgrpcwebjsoncontenttype? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/appfwgrpcwebjsoncontenttype? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of appfwgrpcwebjsoncontenttype resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/appfwgrpcwebjsoncontenttype? **view=summary**

Use this query-parameter to get the summary output of appfwgrpcwebjsoncontenttype resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/appfwgrpcwebjsoncontenttype? **pagesize=#no;pageno=#no**

Use this query-parameter to get the appfwgrpcwebjsoncontenttype resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "appfwgrpcwebjsoncontenttype": [ {

"grpcwebjsoncontenttypevalue":<String_value>,

"isregex":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwgrpcwebjsoncontenttype/ grpcwebjsoncontenttypevalue_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/appfwgrpcwebjsoncontenttype/ grpcwebjsoncontenttypevalue_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/appfwgrpcwebjsoncontenttype/ grpcwebjsoncontenttypevalue_value<String> ? **view=summary**

Use this query-parameter to get the summary output of appfwgrpcwebjsoncontenttype resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwgrpcwebjsoncontenttype": [ {

"grpcwebjsoncontenttypevalue":<String_value>,

"isregex":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwgrpcwebjsoncontenttype? **count=yes**
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "appfwgrpcwebjsoncontenttype": [ { "__count": "#no"} ] }
```

appfwgrpcwebtextcontenttype

Configuration for gRRPC-Web-text content type resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
grpcwebtextcontenttypevalue	<String>	Read-write	Content type to be classified as gRPC-web-text. Minimum length = 1
isregex	<String>	Read-write	Is gRPC-web-text content type a regular expression?. Default value: NOTREGEX Possible values = REGEX, NOTREGEX

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwgrpcwebtextcontenttype **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"appfwgrpcwebtextcontenttype":{

<b>"grpcwebtextcontenttypevalue":<String_value>,

</b>"isregex":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwgrpcwebtextcontenttype/grpcwebtextcontenttypevalue_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwgrpcwebtextcontenttype **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/appfwgrpcwebtextcontenttype? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/appfwgrpcwebtextcontenttype? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of appfwgrpcwebtextcontenttype resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/appfwgrpcwebtextcontenttype? **view=summary**

Use this query-parameter to get the summary output of appfwgrpcwebtextcontenttype resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/appfwgrpcwebtextcontenttype? **pagesize=#no;pageno=#no**

Use this query-parameter to get the appfwgrpcwebtextcontenttype resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "appfwgrpcwebtextcontenttype": [ {

"grpcwebtextcontenttypevalue":<String_value>,

"isregex":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwgrpcwebtextcontenttype/ grpcwebtextcontenttypevalue_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/appfwgrpcwebtextcontenttype/ grpcwebtextcontenttypevalue_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/appfwgrpcwebtextcontenttype/ grpcwebtextcontenttypevalue_value<String> ? **view=summary**

Use this query-parameter to get the summary output of appfwgrpcwebtextcontenttype resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwgrpcwebtextcontenttype": [ {

"grpcwebtextcontenttypevalue":<String_value>,

"isregex":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwgrpcwebtextcontenttype? **count=yes**
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "appfwgrpcwebtextcontenttype": [ { "__count": "#no"} ] }
```

appfwhtmlerrorpage

Configuration for HTML error page resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the XML error object to remove. Minimum length = 1
src	<String>	Read-write	URL (protocol, host, path, and name) for the location from which to fetch the imported HTML error object. NOTE: The import fails if the object to be imported is on an HTTPS server that requires client certificate authentication for access. Minimum length = 1 Maximum length = 2047
comment	<String>	Read-write	Any comments to preserve information about the HTML error object. Maximum length = 128
overwrite	<Boolean>	Read-write	Overwrite any existing HTML error object of the same name.
response	<String>	Read-only	.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- DELETE
- GET (ALL)
- GET
- IMPORT
- CHANGE

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwhtmlerrorpage/ name_value<String>
HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

IMPORT

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwhtmlerrorpage? **action=Import HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"appfwhtmlerrorpage":{

<b>"src":<String_value>,

</b><b>"name":<String_value>,

</b>"comment":<String_value>,

"overwrite":<Boolean_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

CHANGE

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwhtmlerrorpage? **action=update HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"appfwhtmlerrorpage":{

<b>"name":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwhtmlerrorpage **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "appfwhtmlerrorpage": [ {

"name":<String_value>,

"response":<String_value>,

"src":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwhtmlerrorpage/ name_value<String>
Query-parameters: attrs http:// <netscaler-ip-address> /nitro/v1/config/appfwhtmlerrorpage/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/appfwhtmlerrorpage/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of appfwhtmlerrorpage resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwhtmlerrorpage": [ {

"name":<String_value>,

"response":<String_value>,

"src":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

appfwjsoncontenttype

Configuration for JSON content type resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
jsoncontenttypevalue	<String>	Read-write	Content type to be classified as JSON. Minimum length = 1
isregex	<String>	Read-write	Is json content type a regular expression?. Default value: NOTREGEX Possible values = REGEX, NOTREGEX
builtin	<String[]>	Read-only	Flag to determine if jsoncontenttype is built-in or not.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL
feature	<String>	Read-only	The feature to be checked while applying this config.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwjsoncontenttype **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"appfwjsoncontenttype":{

<b>"jsoncontenttypevalue":<String_value>,

</b>"isregex":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwjsoncontenttype/ jsoncontenttypevalue_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwjsoncontenttype **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/appfwjsoncontenttype? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/appfwjsoncontenttype? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of appfwjsoncontenttype resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/appfwjsoncontenttype? **view=summary**

Use this query-parameter to get the summary output of appfwjsoncontenttype resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/appfwjsoncontenttype? **pagesize=#no;pageno=#no**

Use this query-parameter to get the appfwjsoncontenttype resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "appfwjsoncontenttype": [ {

"jsoncontenttypevalue":<String_value>,

"isregex":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwjsoncontenttype/ jsoncontenttypevalue_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> / nitro/v1/config/appfwjsoncontenttype/ jsoncontenttypevalue_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/appfwjsoncontenttype/ jsoncontenttypevalue_value<String> ? **view=summary**

Use this query-parameter to get the summary output of appfwjsoncontenttype resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwjsoncontenttype": [ {

"jsoncontenttypevalue":<String_value>,

"isregex":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwjsoncontenttype? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "appfwjsoncontenttype": [ { "__count": "#no"} ] }
```

appfwjsonerrorpage

Configuration for JSON error page resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Indicates name of the imported json error page to be removed. Minimum length = 1
src	<String>	Read-write	URL (protocol, host, path, and name) for the location from which to fetch the imported JSON error object. NOTE: The import fails if the object to be imported is on an HTTPS server that requires client certificate authentication for access. Minimum length = 1 Maximum length = 2047

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
comment	<String>	Read-write	Any comments to preserve information about the JSON error object. Maximum length = 128
overwrite	<Boolean>	Read-write	Overwrite any existing JSON error object of the same name.
response	<String>	Read-only	JSON error object contents.
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- DELETE
- GET (ALL)
- GET
- IMPORT
- CHANGE

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwjsonerrorpage/ name_value<String>
HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

IMPORT

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwjsonerrorpage? **action=Import HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"appfwjsonerrorpage":{

<b>"src":<String_value>,

</b><b>"name":<String_value>,

</b>"comment":<String_value>,

"overwrite":<Boolean_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

CHANGE

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwjsonerrorpage? **action=update HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"appfwjsonerrorpage":{

<b>"name":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwjsonerrorpage **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "appfwjsonerrorpage": [ {

"name":<String_value>,

"response":<String_value>,

"src":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwjsonerrorpage/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/appfwjsonerrorpage/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/appfwjsonerrorpage/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of appfwjsonerrorpage resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwjsonerrorpage": [ {

"name":<String_value>,

"response":<String_value>,

"src":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

appfwlearningdata

Configuration for learning data resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
profilename	<String>	Read-write	Name of the profile.
starturl	<String>	Read-write	Start URL configuration. Minimum length = 1
cookieconsistency	<String>	Read-write	Cookie Name. Minimum length = 1
fieldconsistency	<String>	Read-write	Form field name. Minimum length = 1
formactionurl_ffc	<String>	Read-write	Form action URL.
contenttype	<String>	Read-write	Content Type Name. Minimum length = 1
crosssitescripting	<String>	Read-write	Cross-site scripting. Minimum length = 1
formactionurl_xss	<String>	Read-write	Form action URL. Minimum length = 1
as_scan_location_xss	<String>	Read-write	Location of cross-site scripting exception - form field, header, cookie or url. Possible values = FORMFIELD, HEADER, COOKIE, URL
as_value_type_xss	<String>	Read-write	XSS value type. (Tag | Attribute | Pattern). Possible values = Tag, Attribute, Pattern

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
as_value_expr_xss	<String>	Read-write	XSS value expressions consistituting expressions for Tag, Attribute or Pattern.
sqlinjection	<String>	Read-write	Form field name. Minimum length = 1
formactionurl_sql	<String>	Read-write	Form action URL. Minimum length = 1
as_scan_location_sql	<String>	Read-write	Location of sql injection exception - form field, header or cookie. Possible values = FORMFIELD, HEADER, COOKIE
as_value_type_sql	<String>	Read-write	SQL value type. Keyword, SpecialString or Wildchar. Possible values = Keyword, SpecialString, Wildchar
as_value_expr_sql	<String>	Read-write	SQL value expressions consistituting expressions for Keyword, SpecialString or Wildchar.
fieldformat	<String>	Read-write	Field format name. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
formactionurl_ff	<String>	Read-write	Form action URL. Minimum length = 1
csrftag	<String>	Read-write	CSRF Form Action URL. Minimum length = 1
csrfformoriginurl	<String>	Read-write	CSRF Form Origin URL. Minimum length = 1
creditcardnumber	<String>	Read-write	The object expression that is to be excluded from safe commerce check. Minimum length = 1
creditcardnumberurl	<String>	Read-write	The url for which the list of credit card numbers are needed to be bypassed from inspection. Minimum length = 1
xmldoscheck	<String>	Read-write	XML Denial of Service check, one of MaxAttributes MaxAttributeNameLength MaxAttributeValueLength MaxElementNameLength MaxFileSize

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			MinFileSize MaxCDATALength MaxElements MaxElementDepth MaxElementChildren NumDTDs NumProcessingInstructions NumExternalEntities MaxEntityExpansions MaxEntityExpansionDepth MaxNamespaces MaxNamespaceUriLength MaxSOAPArraySize MaxSOAPArrayRank . Minimum length = 1
xmlwsicheck	<String>	Read-write	Web Services Interoperability Rule ID.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum length = 1
xmlattachmentcheck	<String>	Read-write	XML Attachment Content-Type. Minimum length = 1
totalxmlrequests	<Boolean>	Read-write	Total XML requests.
securitycheck	<String>	Read-write	Name of the security check. Possible values = startURL, cookieConsistency, fieldConsistency, crossSiteScripting, SQLInjection, fieldFormat, CSRFtag, XMLDoSCheck, XMLWSICheck, XMLAttachmentCheck, TotalXMLRequests, creditCardNumber, ContentType
target	<String>	Read-write	Target filename for data to be exported. Minimum length = 1 Maximum length = 127
url	<String>	Read-only	Learnt url.
name	<String>	Read-only	Learnt field name.
fieldtype	<String>	Read-only	Learnt field type.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
fieldformatminlength	<Integer>	Read-only	The minimum allowed length for data in this form field.
fieldformatmaxlength	<Integer>	Read-only	The maximum allowed length for data in this form field.
fieldformatcharmappcre	<String>	Read-only	Form field value allowed character map.
value_type	<String>	Read-only	Learnt field value type.
value	<String>	Read-only	Learnt field value.
hits	<Integer>	Read-only	Learnt entity hit count.
data	<String>	Read-only	Learned data.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- DELETE
- GET (ALL)
- COUNT
- RESET
- EXPORT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwlearningdata **Query-parameters: args= profilename:<String_value>, starturl: <String_value> ,cookieconsistency: <String_value> ,fieldconsistency: <String_value> ,formactionurl_ffc: <String_value> ,contenttype: <String_value> ,crosssitescripting: <String_value> ,formactionurl_xss: <String_value> ,as_scan_location_xss: <String_value> ,as_value_type_xss: <String_value> ,as_value_expr_xss: <String_value> ,sqlinjection: <String_value> ,formactionurl_sql: <String_value> ,as_scan_location_sql: <String_value> ,as_value_type_sql: <String_value> ,as_value_expr_sql: <String_value> ,fieldformat: <String_value> ,formactionurl_ff: <String_value> ,csrftag: <String_value> ,csrfformoriginurl: <String_value> ,creditcardnumber: <String_value> ,creditcardnumberurl: <String_value> ,xmldoscheck: <String_value> ,xmlwsicheck: <String_value> ,xmlattachmentcheck: <String_value> ,totalxmlrequests: <Boolean_value>** reset

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwlearningdata? **action=reset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"appfwlearningdata":{

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

export

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwlearningdata? **action=export HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"appfwlearningdata":{

<b>"profilename":<String_value>,

</b><b>"securitycheck":<String_value>,

</b>"target":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error
get (all)
URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwlearningdata **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/appfwlearningdata? **args= profilename:<String_value>, securitycheck:<String_value>,**

Use this query-parameter to get appfwlearningdata resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/config/appfwlearningdata? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/appfwlearningdata? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of appfwlearningdata resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/appfwlearningdata? **view=summary**

Use this query-parameter to get the summary output of appfwlearningdata resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/appfwlearningdata? **pagesize=#no;pageno=#no**

Use this query-parameter to get the appfwlearningdata resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "appfwlearningdata": [ {

<b>profilename:<String_value>,</b><b>securitycheck:<String_value>,</
b>"url":<String_value>,

"name":<String_value>,

"fieldtype":<String_value>,

"fieldformatminlength":<Integer_value>,

"fieldformatmaxlength":<Integer_value>,

"fieldformatcharmappcre":<String_value>,

"value_type":<String_value>,

"value":<String_value>,

"hits":<Integer_value>,

"data":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

count

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwlearningdata? **args= profilename:<String_value>, securitycheck:<String_value>, ;count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "appfwlearningdata": [ { "__count": "#no"} ] }
```

appfwlearningsettings

Configuration for learning settings resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
profilename	<String>	Read-write	Name of the profile. Minimum length = 1
starturlminthreshold	<Integer>	Read-write	Minimum number of application firewall sessions that the learning engine must observe to learn start URLs. Default value: 1 Minimum value = 1
starturlpercentthreshold	<Integer>	Read-write	Minimum percentage of application firewall sessions that must

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			contain a particular start URL pattern for the learning engine to learn that start URL. Default value: 0 Minimum value = 0 Maximum value = 100
cookieconsistencyminthreshold	<Integer>	Read-write	Minimum number of application firewall sessions that the learning engine must observe to learn cookies. Default value: 1 Minimum value = 1
cookieconsistencypercentthreshold	<Integer>	Read-write	Minimum percentage of application firewall sessions that must contain a particular cookie pattern for the learning engine to learn that cookie. Default value: 0 Minimum value = 0 Maximum value = 100
csrftagminthreshold	<Integer>	Read-write	Minimum number of application firewall sessions that the learning engine must observe to learn

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			cross-site request forgery (CSRF) tags. Default value: 1 Minimum value = 1
csrftagpercentthreshold	<Integer>	Read-write	Minimum percentage of application firewall sessions that must contain a particular CSRF tag for the learning engine to learn that CSRF tag. Default value: 0 Minimum value = 0 Maximum value = 100
fieldconsistencymintthreshold	<Integer>	Read-write	Minimum number of application firewall sessions that the learning engine must observe to learn field consistency information. Default value: 1 Minimum value = 1
fieldconsistencypercentthreshold	<Integer>	Read-write	Minimum percentage of application firewall sessions that must contain a particular field consistency pattern for the learning engine to learn that field consistency pattern.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: 0 Minimum value = 0 Maximum value = 100
crosssitescriptingminthreshold	<Integer>	Read-write	Minimum number of application firewall sessions that the learning engine must observe to learn HTML cross-site scripting patterns. Default value: 1 Minimum value = 1
crosssitescriptingpercentthreshold	<Integer>	Read-write	Minimum percentage of application firewall sessions that must contain a particular cross-site scripting pattern for the learning engine to learn that cross-site scripting pattern. Default value: 0 Minimum value = 0 Maximum value = 100
sqlinjectionminthreshold	<Integer>	Read-write	Minimum number of application firewall sessions that the learning engine must observe to learn HTML SQL injection patterns.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: 1 Minimum value = 1
sqlinjectionpercentthreshold	<Integer>	Read-write	Minimum percentage of application firewall sessions that must contain a particular HTML SQL injection pattern for the learning engine to learn that HTML SQL injection pattern. Default value: 0 Minimum value = 0 Maximum value = 100
fieldformatminthreshold	<Integer>	Read-write	Minimum number of application firewall sessions that the learning engine must observe to learn field formats. Default value: 1 Minimum value = 1
fieldformatpercentthreshold	<Integer>	Read-write	Minimum percentage of application firewall sessions that must contain a particular web form field pattern for the learning engine to recommend a field format for that form field.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: 0 Minimum value = 0 Maximum value = 100
creditcardnumbermin threshold	<Integer>	Read-write	Minimum threshold to learn Credit Card information. Default value: 1 Minimum value = 1
creditcardnumberper centthreshold	<Integer>	Read-write	Minimum threshold in percent to learn Credit Card information. Default value: 0 Minimum value = 0 Maximum value = 100
contenttypeminthres hold	<Integer>	Read-write	Minimum threshold to learn Content Type information. Default value: 1 Minimum value = 1
contenttypepercentth reshold	<Integer>	Read-write	Minimum threshold in percent to learn Content Type information. Default value: 0 Minimum value = 0

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum value = 100
xmlwsiminthreshold	<Integer>	Read-write	Minimum number of application firewall sessions that the learning engine must observe to learn web services interoperability (WSI) information. Default value: 1 Minimum value = 1
xmlwsipercentthreshold	<Integer>	Read-write	Minimum percentage of application firewall sessions that must contain a particular pattern for the learning engine to learn a web services interoperability (WSI) pattern. Default value: 0 Minimum value = 0 Maximum value = 100
xmlattachmentminthreshold	<Integer>	Read-write	Minimum number of application firewall sessions that the learning engine must observe to learn XML attachment patterns. Default value: 1 Minimum value = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
xmlattachmentpercentthreshold	<Integer>	Read-write	Minimum percentage of application firewall sessions that must contain a particular XML attachment pattern for the learning engine to learn that XML attachment pattern. Default value: 0 Minimum value = 0 Maximum value = 100
fieldformatautodeploygraceperiod	<Integer>	Read-write	The number of minutes after the threshold hit alert the learned rule will be deployed. Default value: 10080 Minimum value = 5 Maximum value = 43200
sqlinjectionautodeploygraceperiod	<Integer>	Read-write	The number of minutes after the threshold hit alert the learned rule will be deployed. Default value: 10080 Minimum value = 5

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum value = 43200
crosssitescriptingautodeploygraceperiod	<Integer>	Read-write	The number of minutes after the threshold hit alert the learned rule will be deployed. Default value: 10080 Minimum value = 5 Maximum value = 43200
starturlautodeploygraceperiod	<Integer>	Read-write	The number of minutes after the threshold hit alert the learned rule will be deployed. Default value: 10080 Minimum value = 5 Maximum value = 43200
cookieconsistencyautodeploygraceperiod	<Integer>	Read-write	The number of minutes after the threshold hit alert the learned rule will be deployed. Default value: 10080 Minimum value = 5

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum value = 43200
csrftagautodeploygraceperiod	<Integer>	Read-write	The number of minutes after the threshold hit alert the learned rule will be deployed. Default value: 10080 Minimum value = 5 Maximum value = 43200
fieldconsistencyautodeploygraceperiod	<Integer>	Read-write	The number of minutes after the threshold hit alert the learned rule will be deployed. Default value: 10080 Minimum value = 5 Maximum value = 43200
contenttypeautodeploygraceperiod	<Integer>	Read-write	The number of minutes after the threshold hit alert the learned rule will be deployed. Default value: 10080 Minimum value = 5

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum value = 43200
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwlearningsettings **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"appfwlearningsettings":{

<b>"profilename":<String_value>,

</b>"starturlminthreshold":<Integer_value>,

"starturlpercentthreshold":<Integer_value>,

"cookieconsistencyminthreshold":<Integer_value>,

"cookieconsistencypercentthreshold":<Integer_value>,

"csrftagminthreshold":<Integer_value>,

"csrftagpercentthreshold":<Integer_value>,

"fieldconsistencyminthreshold":<Integer_value>,

"fieldconsistencypercentthreshold":<Integer_value>,

"crosssitescriptingminthreshold":<Integer_value>,

"crosssitescriptingpercentthreshold":<Integer_value>,

"sqlinjectionminthreshold":<Integer_value>,

"sqlinjectionpercentthreshold":<Integer_value>,

"fieldformatminthreshold":<Integer_value>,
```

```
"fieldformatpercentthreshold":<Integer_value>,

"creditcardnumberminthreshold":<Integer_value>,

"creditcardnumberpercentthreshold":<Integer_value>,

"contenttypeminthreshold":<Integer_value>,

"contenttypepercentthreshold":<Integer_value>,

"xmlwsiminthreshold":<Integer_value>,

"xmlwsipercentthreshold":<Integer_value>,

"xmlattachmentminthreshold":<Integer_value>,

"xmlattachmentpercentthreshold":<Integer_value>,

"fieldformatautodeploygraceperiod":<Integer_value>,

"sqlinjectionautodeploygraceperiod":<Integer_value>,

"crosssitescriptingautodeploygraceperiod":<Integer_value>,

"starturlautodeploygraceperiod":<Integer_value>,

"cookieconsistencyautodeploygraceperiod":<Integer_value>,

"csrftagautodeploygraceperiod":<Integer_value>,

"fieldconsistencyautodeploygraceperiod":<Integer_value>,

"contenttypeautodeploygraceperiod":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwlearningsettings? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"appfwlearningsettings":{

<b>"profilename":<String_value>,

</b>"starturlminthreshold":true,

"starturlpercentthreshold":true,

"cookieconsistencyminthreshold":true,

"cookieconsistencypercentthreshold":true,

"csrftagminthreshold":true,

"csrftagpercentthreshold":true,

"fieldconsistencyminthreshold":true,

"fieldconsistencypercentthreshold":true,

"crosssitescriptingminthreshold":true,

"crosssitescriptingpercentthreshold":true,

"sqlinjectionminthreshold":true,

"sqlinjectionpercentthreshold":true,

"fieldformatminthreshold":true,

"fieldformatpercentthreshold":true,
```

```
"creditcardnumberminthreshold":true,

"creditcardnumberpercentthreshold":true,

"contenttypeminthreshold":true,

"contenttypepercentthreshold":true,

"xmlwsiminthreshold":true,

"xmlwsipercentthreshold":true,

"xmlattachmentminthreshold":true,

"xmlattachmentpercentthreshold":true,

"fieldformatautodeploygraceperiod":true,

"sqlinjectionautodeploygraceperiod":true,

"crosssitescriptingautodeploygraceperiod":true,

"starturlautodeploygraceperiod":true,

"cookieconsistencyautodeploygraceperiod":true,

"csrftagautodeploygraceperiod":true,

"fieldconsistencyautodeploygraceperiod":true,

"contenttypeautodeploygraceperiod":true

}}
```


Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwlearningsettings **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/appfwlearningsettings? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/appfwlearningsettings? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of appfwlearningsettings resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/appfwlearningsettings? **view=summary**

Use this query-parameter to get the summary output of appfwlearningsettings resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/appfwlearningsettings? **pagesize=#no;pageno=#no**

Use this query-parameter to get the appfwlearningsettings resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "appfwlearningsettings": [ {

"profilename":<String_value>,

"starturlminthreshold":<Integer_value>,

"starturlpercentthreshold":<Integer_value>,

"cookieconsistencyminthreshold":<Integer_value>,

"cookieconsistencypercentthreshold":<Integer_value>,

"csrftagminthreshold":<Integer_value>,

"csrftagpercentthreshold":<Integer_value>,

"fieldconsistencyminthreshold":<Integer_value>,

"fieldconsistencypercentthreshold":<Integer_value>,

"crosssitescriptingminthreshold":<Integer_value>,

"crosssitescriptingpercentthreshold":<Integer_value>,

"sqlinjectionminthreshold":<Integer_value>,

"sqlinjectionpercentthreshold":<Integer_value>,

"fieldformatminthreshold":<Integer_value>,

"fieldformatpercentthreshold":<Integer_value>,

"creditcardnumberminthreshold":<Integer_value>,

"creditcardnumberpercentthreshold":<Integer_value>,

"contenttypeminthreshold":<Integer_value>,

"contenttypepercentthreshold":<Integer_value>,

"xmlwsiminthreshold":<Integer_value>,

"xmlwsipercentthreshold":<Integer_value>,
```

```
"xmlattachmentminthreshold":<Integer_value>,

"xmlattachmentpercentthreshold":<Integer_value>,

"crosssitescriptingautodeploygraceperiod":<Integer_value>,

"sqlinjectionautodeploygraceperiod":<Integer_value>,

"fieldformatautodeploygraceperiod":<Integer_value>,

"starturlautodeploygraceperiod":<Integer_value>,

"cookieconsistencyautodeploygraceperiod":<Integer_value>,

"csrftagautodeploygraceperiod":<Integer_value>,

"fieldconsistencyautodeploygraceperiod":<Integer_value>,

"contenttypeautodeploygraceperiod":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwlearningsettings/ profilename_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/ config/appfwlearningsettings/ profilename_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/appfwlearningsettings/ profilename_value<String> ? **view=summary**

Use this query-parameter to get the summary output of appfwlearningsettings resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwlearningsettings": [ {

"profilename":<String_value>,

"starturlminthreshold":<Integer_value>,

"starturlpercentthreshold":<Integer_value>,

"cookieconsistencyminthreshold":<Integer_value>,

"cookieconsistencypercentthreshold":<Integer_value>,

"csrftagminthreshold":<Integer_value>,

"csrftagpercentthreshold":<Integer_value>,

"fieldconsistencyminthreshold":<Integer_value>,

"fieldconsistencypercentthreshold":<Integer_value>,

"crosssitescriptingminthreshold":<Integer_value>,

"crosssitescriptingpercentthreshold":<Integer_value>,

"sqlinjectionminthreshold":<Integer_value>,

"sqlinjectionpercentthreshold":<Integer_value>,
```

```
"fieldformatminthreshold":<Integer_value>,

"fieldformatpercentthreshold":<Integer_value>,

"creditcardnumberminthreshold":<Integer_value>,

"creditcardnumberpercentthreshold":<Integer_value>,

"contenttypeminthreshold":<Integer_value>,

"contenttypepercentthreshold":<Integer_value>,

"xmlwsiminthreshold":<Integer_value>,

"xmlwsipercentthreshold":<Integer_value>,

"xmlattachmentminthreshold":<Integer_value>,

"xmlattachmentpercentthreshold":<Integer_value>,

"crosssitescriptingautodeploygraceperiod":<Integer_value>,

"sqlinjectionautodeploygraceperiod":<Integer_value>,

"fieldformatautodeploygraceperiod":<Integer_value>,

"starturlautodeploygraceperiod":<Integer_value>,

"cookieconsistencyautodeploygraceperiod":<Integer_value>,

"csrftagautodeploygraceperiod":<Integer_value>,

"fieldconsistencyautodeploygraceperiod":<Integer_value>,

"contenttypeautodeploygraceperiod":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwlearningsettings? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "appfwlearningsettings": [ { "__count": "#no"} ] }
```

appfwmultipartformcontenttype

Configuration for Multipart form content type resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
multipartformcontenttypevalue	<String>	Read-write	Content type to be classified as multipart form. Minimum length = 1
isregex	<String>	Read-write	Is multipart_form content type a regular expression?.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: NOTREGEX Possible values = REGEX, NOTREGEX
builtin	<String[]>	Read-only	Flag to determine if multipart form contenttype is built-in or not. Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL
feature	<String>	Read-only	The feature to be checked while applying this config.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwmultipartformcontenttype **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"appfwmultipartformcontenttype":{

<b>"multipartformcontenttypevalue":<String_value>,

</b>"isregex":<String_value>
```

```
}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwmultipartformcontenttype/ multipartformcontenttypevalue_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwmultipartformcontenttype **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/appfwmultipartformcontenttype? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/appfwmultipartformcontenttype? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of appfwmultipartformcontenttype resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/appfwmultipartformcontenttype? **view=summary**

Use this query-parameter to get the summary output of appfwmultipartformcontenttype resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/appfwmultipartformcontenttype? **pagesize=#no;pageno=#no**

Use this query-parameter to get the appfwmultipartformcontenttype resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "appfwmultipartformcontenttype": [ {

"multipartformcontenttypevalue":<String_value>,

"isregex":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwmultipartformcontenttype/ multipartformcontenttypevalue_value<String> **Query-parameters: attrs** http:// <netscaler-ip-

address> /nitro/v1/config/appfwmultipartformcontenttype/ multipartformcontenttypevalue_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/appfwmultipartformcontenttype/ multipartformcontenttypevalue_value<String> ? **view=summary**

Use this query-parameter to get the summary output of appfwmultipartformcontenttype resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwmultipartformcontenttype": [ {

"multipartformcontenttypevalue":<String_value>,

"isregex":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

```
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwmultipartformcontenttype? **count=yes**
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "appfwmultipartformcontenttype": [ { "__count": "#no"} ] }
```

appfwpolicy

Configuration for application firewall policy resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the policy. Must begin with a letter, number, or the underscore character \(_\), and must contain only letters, numbers,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			and the hyphen \(-\), period \(.\) pound \(#\), space \(\), at (@), equals \(=\), colon \(:\), and underscore characters. Can be changed after the policy is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks \(for example, "my policy" or 'my policy'\). Minimum length = 1
rule	<String>	Read-write	Name of the Citrix ADC named rule, or a Citrix ADC expression, that the policy uses to determine whether to filter the connection through the application firewall with the designated profile.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
profilename	<String>	Read-write	Name of the application firewall profile to use if the policy matches. Minimum length = 1
comment	<String>	Read-write	Any comments to preserve information about the policy for later reference.
logaction	<String>	Read-write	Where to log information for connections that match this policy.
newname	<String>	Read-write	New name for the policy. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			"my policy" or 'my policy'). Minimum length = 1
hits	<Integer>	Read-only	Number of hits.
undefhits	<Integer>	Read-only	Number of Undef hits.
policytype	<String>	Read-only	. Possible values = Classic Policy, Advanced Policy
builtin	<String[]>	Read-only	Flag to determine if application firewall policy is built-in or not. Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL
feature	<String>	Read-only	The feature to be checked while applying this config.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE

- UNSET
- GET (ALL)
- GET
- COUNT
- RENAME

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwpolicy **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"appfwpolicy":{

<b>"name":<String_value>,

</b><b>"rule":<String_value>,

</b><b>"profilename":<String_value>,

</b>"comment":<String_value>,

"logaction":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwpolicy/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwpolicy **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"appfwpolicy":{

<b>"name":<String_value>,

</b>"rule":<String_value>,

"profilename":<String_value>,

"comment":<String_value>,

"logaction":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwpolicy? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"appfwpolicy":{

<b>"name":<String_value>,

</b>"comment":true,

"logaction":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

RENAME

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwpolicy? **action=rename HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"appfwpolicy":{

<b>"name":<String_value>,

</b><b>"newname":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwpolicy **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/appfwpolicy? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/appfwpolicy? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of appfwpolicy resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/appfwpolicy? **view=summary**

Use this query-parameter to get the summary output of appfwpolicy resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/appfwpolicy? **pagesize=#no;pageno=#no**

Use this query-parameter to get the appfwpolicy resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "appfwpolicy": [ {

"name":<String_value>,

"rule":<String_value>,

"profilename":<String_value>,

"hits":<Integer_value>,

"undefhits":<Integer_value>,
```

```
"comment":<String_value>,

"logaction":<String_value>,

"policytype":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwpolicy/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/appfwpolicy/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/appfwpolicy/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of appfwpolicy resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwpolicy": [ {

"name":<String_value>,

"rule":<String_value>,

"profilename":<String_value>,

"hits":<Integer_value>,

"undefhits":<Integer_value>,

"comment":<String_value>,

"logaction":<String_value>,

"policytype":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwpolicy? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "appfwpolicy": [ { "__count": "#no"} ] }
```

appfwpolicy_appfwglobal_binding

Binding object showing the appfwglobal that can be bound to appfwpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the policy. Minimum length = 1
boundto	<String>	Read-write	The entity name to which policy is bound.
labeltype	<String>	Read-only	Type of policy label invocation. Possible values = reqvserver, resvserver, policylabel
priority	<Integer>	Read-only	Specifies the priority of the policy.
labelname	<String>	Read-only	Name of the label to invoke if the current policy rule evaluates to TRUE.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
gotopriorityexpression	<String>	Read-only	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
activepolicy	<Integer>	Read-only	Indicates whether policy is bound or not.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwpolicy_appfwglobal_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ appfwpolicy_appfwglobal_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of appfwpolicy_appfwglobal_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/appfwpolicy_appfwglobal_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the appfwpolicy_appfwglobal_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwpolicy_appfwglobal_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"labelname":<String_value>,

"gotopriorityexpression":<String_value>,

"activepolicy":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwpolicy_appfwglobal_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/appfwpolicy_appfwglobal_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwpolicy_appfwglobal_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"labelname":<String_value>,

"gotopriorityexpression":<String_value>,

"activepolicy":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwpolicy_appfwglobal_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"appfwpolicy_appfwglobal_binding": [ { "__count": "#no"} ] }
```

appfwpolicy_appfwpolicylabel_binding

Binding object showing the appfwpolicylabel that can be bound to appfwpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the policy. Minimum length = 1
boundto	<String>	Read-write	The entity name to which policy is bound.
activepolicy	<Integer>	Read-only	Indicates whether policy is bound or not.
gotopriorityexpression	<String>	Read-only	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
labelname	<String>	Read-only	Name of the label to invoke if the current policy rule evaluates to TRUE.
priority	<Integer>	Read-only	Specifies the priority of the policy.
labeltype	<String>	Read-only	Type of policy label invocation.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = reqvserver, resvserver, policylabel
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwpolicy_appfwpolicylabel_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ appfwpolicy_appfwpolicylabel_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of appfwpolicy_appfwpolicylabel_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/appfwpolicy_appfwpolicylabel_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the appfwpolicy_appfwpolicylabel_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwpolicy_appfwpolicylabel_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"activepolicy":<Integer_value>,

"gotopriorityexpression":<String_value>,
```

```
"labelname":<String_value>,

"priority":<Integer_value>,

"labeltype":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwpolicy_appfwpolicylabel_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/appfwpolicy_appfwpolicylabel_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwpolicy_appfwpolicylabel_binding": [ {

"name":<String_value>,

"boundto":<String_value>,
```

```
"activepolicy":<Integer_value>,

"gotopriorityexpression":<String_value>,

"labelname":<String_value>,

"priority":<Integer_value>,

"labeltype":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwpolicy_appfwpolicylabel_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"appfwpolicy_appfwpolicylabel_binding": [ { "__count": "#no"} ] }
```

appfwpolicy_binding

Binding object which returns the resources bound to appfwpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the policy. Minimum length = 1
appfwpolicy_vpnvserver_binding	<appfwpolicy_vpnvserver_binding[]>	Read-only	vpnvserver that can be bound to appfwpolicy.
appfwpolicy_csvserver_binding	<appfwpolicy_csvserver_binding[]>	Read-only	csvserver that can be bound to appfwpolicy.
appfwpolicy_appfwpolicylabel_binding	<appfwpolicy_appfwpolicylabel_binding[]>	Read-only	appfwpolicylabel that can be bound to appfwpolicy.
appfwpolicy_lbvserver_binding	<appfwpolicy_lbvserver_binding[]>	Read-only	lbvserver that can be bound to appfwpolicy.
appfwpolicy_appfwglobal_binding	<appfwpolicy_appfwglobal_binding[]>	Read-only	appfwglobal that can be bound to appfwpolicy.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwpolicy_binding/ name_value<String>
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "appfwpolicy_binding": [ {

"name":<String_value>,
```

```
"appfwpolicy_csvserver_binding":<appfwpolicy_csvserver_binding[]_value>,

"appfwpolicy_vpnvserver_binding":<appfwpolicy_vpnvserver_binding[]_value>,

"appfwpolicy_appfwglobal_binding":<appfwpolicy_appfwglobal_binding[]_value
>,

"appfwpolicy_lbvserver_binding":<appfwpolicy_lbvserver_binding[]_value>,

"appfwpolicy_appfwpolicylabel_binding":<appfwpolicy_appfwpolicylabel_bindi
ng[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwpolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/appfwpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "appfwpolicy_binding": [ {

"name":<String_value>,

"appfwpolicy_csvserver_binding":<appfwpolicy_csvserver_binding[]_value>,

"appfwpolicy_vpnvserver_binding":<appfwpolicy_vpnvserver_binding[]_value>,

"appfwpolicy_appfwglobal_binding":<appfwpolicy_appfwglobal_binding[]_value
>,

"appfwpolicy_lbvserver_binding":<appfwpolicy_lbvserver_binding[]_value>,

"appfwpolicy_appfwpolicylabel_binding":<appfwpolicy_appfwpolicylabel_bindi
ng[]_value>

}]}
```

appfwpolicy_csvserver_binding

Binding object showing the csvserver that can be bound to appfwpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the policy. Minimum length = 1
boundto	<String>	Read-write	The entity name to which policy is bound.
labeltype	<String>	Read-only	Type of policy label invocation. Possible values = reqvserver, resvserver, policylabel

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
priority	<Integer>	Read-only	Specifies the priority of the policy.
labelname	<String>	Read-only	Name of the label to invoke if the current policy rule evaluates to TRUE.
gotopriorityexpression	<String>	Read-only	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
activepolicy	<Integer>	Read-only	Indicates whether policy is bound or not.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwpolicy_csvserver_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ appfwpolicy_csvserver_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of appfwpolicy_csvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/appfwpolicy_csvserver_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the appfwpolicy_csvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwpolicy_csvserver_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"labelname":<String_value>,

"gotopriorityexpression":<String_value>,

"activepolicy":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwpolicy_csvserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/appfwpolicy_csvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwpolicy_csvserver_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"labelname":<String_value>,

"gotopriorityexpression":<String_value>,

"activepolicy":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwpolicy_csvserver_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"appfwpolicy_csvserver_binding": [ { "__count": "#no"} ] }
```

appfwpolicy_lbvserver_binding

Binding object showing the lbvserver that can be bound to appfwpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
boundto	<String>	Read-write	The entity name to which policy is bound.
name	<String>	Read-write	Name of the policy. Minimum length = 1
activepolicy	<Integer>	Read-only	Indicates whether policy is bound or not.
gotopriorityexpression	<String>	Read-only	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
labelname	<String>	Read-only	Name of the label to invoke if the current policy rule evaluates to TRUE.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
priority	<Integer>	Read-only	Specifies the priority of the policy.
labeltype	<String>	Read-only	Type of policy label invocation. Possible values = reqvserver, resvserver, policylabel
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwpolicy_lbvserver_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ appfwpolicy_lbvserver_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of appfwpolicy_lbvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/appfwpolicy_lbvserver_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the appfwpolicy_lbvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwpolicy_lbvserver_binding": [ {

"boundto":<String_value>,
```

```
"name":<String_value>,

"activepolicy":<Integer_value>,

"gotopriorityexpression":<String_value>,

"labelname":<String_value>,

"priority":<Integer_value>,

"labeltype":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwpolicy_lbvserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/appfwpolicy_lbvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwpolicy_lbvserver_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"activepolicy":<Integer_value>,

"gotopriorityexpression":<String_value>,

"labelname":<String_value>,

"priority":<Integer_value>,

"labeltype":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwpolicy_lbvserver_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"appfwpolicy_lbvserver_binding": [ { "__count": "#no"} ] }
```

appfwpolicy_vpnvserver_binding

Binding object showing the vpnvserver that can be bound to appfwpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
boundto	<String>	Read-write	The entity name to which policy is bound.
name	<String>	Read-write	Name of the policy. Minimum length = 1
priority	<Integer>	Read-only	Specifies the priority of the policy.
labeltype	<String>	Read-only	Type of policy label invocation. Possible values = reqvserver, resvserver, policylabel
activepolicy	<Integer>	Read-only	Indicates whether policy is bound or not.
gotopriorityexpression	<String>	Read-only	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
labelname	<String>	Read-only	Name of the label to invoke if the current policy rule evaluates to TRUE.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwpolicy_vpnvserver_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ appfwpolicy_vpnvserver_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of appfwpolicy_vpnvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/appfwpolicy_vpnvserver_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the appfwpolicy_vpnvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwpolicy_vpnvserver_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"priority":<Integer_value>,

"labeltype":<String_value>,

"activepolicy":<Integer_value>,
```

```
"gotopriorityexpression":<String_value>,

"labelname":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwpolicy_vpnvserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/appfwpolicy_vpnvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwpolicy_vpnvserver_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"priority":<Integer_value>,
```

```
"labeltype":<String_value>,

"activepolicy":<Integer_value>,

"gotopriorityexpression":<String_value>,

"labelname":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwpolicy_vpnvserver_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"appfwpolicy_vpnvserver_binding": [ { "__count": "#no"} ] }
```

appfwpolicylabel

Configuration for application firewall policy label resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
labelname	<String>	Read-write	Name for the policy label. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Can be changed after the policy label is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my policy label" or 'my policy label').
policylabeltype	<String>	Read-write	Type of transformations allowed by the policies bound to the label. Always http_req for application firewall policy labels.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = http_req, httpquic_req
newname	<String>	Read-write	The new name of the application firewall policylabel. Minimum length = 1
numpol	<Integer>	Read-only	Number of polices bound to label.
hits	<Integer>	Read-only	Number of times policy label was invoked.
priority	<Integer>	Read-only	Positive integer specifying the priority of the policy. A lower number specifies a higher priority. Must be unique within a group of policies that are bound to the same bind point or label. Policies are evaluated in the order of their priority numbers.
gotopriorityexpression	<String>	Read-only	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
labeltype	<String>	Read-only	Type of policy label to invoke if the current policy

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			evaluates to TRUE and the invoke parameter is set. Available settings function as follows: * reqvserver. Invoke the unnamed policy label associated with the specified request virtual server. * policylabel. Invoke the specified user-defined policy label. Possible values = reqvserver, policylabel
invoke_labelname	<String>	Read-only	Name of the policy label to invoke if the current policy evaluates to TRUE, the invoke parameter is set, and Label Type is set to Policy Label.
description	<String>	Read-only	Description of the policylabel.
policytype	<String>	Read-only	. Possible values = Classic Policy, Advanced Policy
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET (ALL)
- GET
- COUNT
- RENAME

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwpolicylabel **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"appfwpolicylabel":{

<b>"labelname":<String_value>,

</b><b>"policylabeltype":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwpolicylabel/ labelname_value<String>
HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

RENAME

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwpolicylabel? **action=rename HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"appfwpolicylabel":{

<b>"labelname":<String_value>,

</b><b>"newname":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwpolicylabel **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/appfwpolicylabel? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/appfwpolicylabel? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of appfwpolicylabel resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/appfwpolicylabel? **view=summary**

Use this query-parameter to get the summary output of appfwpolicylabel resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/appfwpolicylabel? **pagesize=#no;pageno=#no**

Use this query-parameter to get the appfwpolicylabel resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "appfwpolicylabel": [ {

"labelname":<String_value>,

"policylabeltype":<String_value>,

"numpol":<Integer_value>,

"hits":<Integer_value>,

"priority":<Integer_value>,

"gotopriorityexpression":<String_value>,

"labeltype":<String_value>,

"invoke_labelname":<String_value>,

"description":<String_value>,

"policytype":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwpolicylabel/ labelname_value<String>
Query-parameters: attrs http:// <netscaler-ip-address> /nitro/v1/config/appfwpolicylabel/ labelname_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/appfwpolicylabel/ labelname_value<String> ? **view=summary**

Use this query-parameter to get the summary output of appfwpolicylabel resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwpolicylabel": [ {

"labelname":<String_value>,

"policylabeltype":<String_value>,

"numpol":<Integer_value>,

"hits":<Integer_value>,
```

```
"priority":<Integer_value>,

"gotopriorityexpression":<String_value>,

"labeltype":<String_value>,

"invoke_labelname":<String_value>,

"description":<String_value>,

"policytype":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwpolicylabel? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "appfwpolicylabel": [ { "__count": "#no"} ] }
```

appfwpolicylabel_appfwpolicy_binding

Binding object showing the appfwpolicy that can be bound to appfwpolicylabel.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
labeltype	<String>	Read-write	Type of policy label to invoke if the current policy evaluates to TRUE and the invoke parameter is set. Available settings function as follows: * reqvserver. Invoke the unnamed policy label associated with the specified request virtual server. * policylabel. Invoke the specified user-defined policy label. Possible values = reqvserver, policylabel
priority	<Integer>	Read-write	Positive integer specifying the priority of the policy. A lower number specifies a higher priority. Must be unique within a group of policies that are bound to the same bind point or label. Policies are evaluated in the order of their priority numbers.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
policyname	<String>	Read-write	Name of the application firewall policy to bind to the policy label.
invoke_labelname	<String>	Read-write	Name of the policy label to invoke if the current policy evaluates to TRUE, the invoke parameter is set, and Label Type is set to Policy Label.
labelname	<String>	Read-write	Name of the application firewall policy label.
gotopriorityexpression	<String>	Read-write	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
invoke	<Boolean>	Read-write	If the current policy evaluates to TRUE, terminate evaluation of policies bound to the current policy label, and then forward the request to the specified virtual server or evaluate the specified policy label.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/appfwpolicylabel_appfwpolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"appfwpolicylabel_appfwpolicy_binding":{

<b>"labelname":<String_value>,

</b><b>"policyname":<String_value>,

</b><b>"priority":<Integer_value>,

</b>"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>,

"labeltype":<String_value>,

"invoke_labelname":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwpolicylabel_appfwpolicy_binding/ labelname_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ appfwpolicylabel_appfwpolicy_binding/ labelname_value<String> ? **args= policyname:<String_value>, priority: <Integer_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwpolicylabel_appfwpolicy_binding/ labelname_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ appfwpolicylabel_appfwpolicy_binding/ labelname_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of appfwpolicylabel_appfwpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/appfwpolicylabel_appfwpolicy_binding/ labelname_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the appfwpolicylabel_appfwpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwpolicylabel_appfwpolicy_binding": [ {

"labeltype":<String_value>,

"priority":<Integer_value>,
```

```
"policyname":<String_value>,

"invoke_labelname":<String_value>,

"labelname":<String_value>,

"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwpolicylabel_appfwpolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/appfwpolicylabel_appfwpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwpolicylabel_appfwpolicy_binding": [ {

"labeltype":<String_value>,

"priority":<Integer_value>,

"policyname":<String_value>,

"invoke_labelname":<String_value>,

"labelname":<String_value>,

"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwpolicylabel_appfwpolicy_binding/ labelname_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"appfwpolicylabel_appfwpolicy_binding": [ { "__count": "#no"} ] }
```

appfwpolicylabel_binding

Binding object which returns the resources bound to appfwpolicylabel.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
labelname	<String>	Read-write	Name of the application firewall policy label.
appfwpolicylabel_appfwpolicy_binding	<appfwpolicylabel_appfwpolicy_binding[]>	Read-only	appfwpolicy that can be bound to appfwpolicylabel.
appfwpolicylabel_policybinding_binding	<appfwpolicylabel_policybinding_binding[]>	Read-only	policybinding that can be bound to appfwpolicylabel.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwpolicylabel_binding/ labelname_value<String>

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "appfwpolicylabel_binding": [ {

"labelname":<String_value>,

"appfwpolicylabel_appfwpolicy_binding":<appfwpolicylabel_appfwpolicy_binding[]_value>,
```

```
"appfwpolicylabel_policybinding_binding":<appfwpolicylabel_policybinding_b
inding[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwpolicylabel_binding

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters:

bulkbindings

http:// <netscaler-ip-address> /nitro/v1/config/appfwpolicylabel_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "appfwpolicylabel_binding": [ {

"labelname":<String_value>,

"appfwpolicylabel_appfwpolicy_binding":<appfwpolicylabel_appfwpolicy_binding[]_value>,

"appfwpolicylabel_policybinding_binding":<appfwpolicylabel_policybinding_binding[]_value>

}]}
```

appfwpolicylabel_policybinding_binding

Binding object showing the policybinding that can be bound to appfwpolicylabel.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
invoke_labelname	<String>	Read-write	Name of the policy label to invoke if the current policy evaluates to TRUE, the invoke parameter is set, and Label Type is set to Policy Label.
invoke	<Boolean>	Read-write	If the current policy evaluates to TRUE, terminate evaluation of policies bound to the current policy label, and then forward the request to the specified virtual server or

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			evaluate the specified policy label.
gotopriorityexpression	<String>	Read-write	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
labelname	<String>	Read-write	Name of the application firewall policy label.
priority	<Integer>	Read-write	Positive integer specifying the priority of the policy. A lower number specifies a higher priority. Must be unique within a group of policies that are bound to the same bind point or label. Policies are evaluated in the order of their priority numbers.
labeltype	<String>	Read-write	Type of policy label to invoke if the current policy evaluates to TRUE and the invoke parameter is set. Available settings function as follows: * reqvserver. Invoke the unnamed policy label associated with the specified request

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			virtual server. * policylabel. Invoke the specified user-defined policy label. Possible values = reqvserver, policylabel
policyname	<String>	Read-write	Name of the application firewall policy to bind to the policy label.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwpolicylabel_policybinding_binding/ labelname_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ appfwpolicylabel_policybinding_binding/ labelname_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of appfwpolicylabel_policybinding_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/appfwpolicylabel_policybinding_binding/ labelname_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the appfwpolicylabel_policybinding_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwpolicylabel_policybinding_binding": [ {

"invoke_labelname":<String_value>,

"invoke":<Boolean_value>,

"gotopriorityexpression":<String_value>,

"labelname":<String_value>,

"priority":<Integer_value>,

"labeltype":<String_value>,

"policyname":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwpolicylabel_policybinding_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/appfwpolicylabel_policybinding_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwpolicylabel_policybinding_binding": [ {

"invoke_labelname":<String_value>,

"invoke":<Boolean_value>,

"gotopriorityexpression":<String_value>,

"labelname":<String_value>,

"priority":<Integer_value>,

"labeltype":<String_value>,

"policyname":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwpolicylabel_policybinding_binding/ labelname_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"appfwpolicylabel_policybinding_binding": [ { "__count": "#no"} ] }
```

appfwprofile

Configuration for application firewall profile resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the profile. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.), pound (#), space ( ), at (@), equals (=), colon (:), and underscore (_) characters. Cannot be changed after the profile is added. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			"my profile" or 'my profile'). Minimum length = 1
defaults	<String>	Read-write	Default configuration to apply to the profile. Basic defaults are intended for standard content that requires little further configuration, such as static web site content. Advanced defaults are intended for specialized content that requires significant specialized configuration, such as heavily scripted or dynamic content. CLI users: When adding an application firewall profile, you can set either the defaults or the type, but not both. To set both options, create the profile by using the add appfw profile command, and then use the set appfw profile command to configure the other option.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = basic, advanced, core, cve
starturlaction	<String[]>	Read-write	One or more Start URL actions. Available settings function as follows: * Block - Block connections that violate this security check. * Learn - Use the learning engine to generate a list of exceptions to this security check. * Log - Log violations of this security check. * Stats - Generate statistics for this security check. * None - Disable all actions for this security check. CLI users: To enable one or more actions, type "set appfw profile -startURLaction" followed by the actions to be enabled. To turn off

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			all actions, type "set appfw profile -startURLaction none". Possible values = none, block, learn, log, stats
infercontenttypexmlpayloadaction	<String[]>	Read-write	One or more infer content type payload actions. Available settings function as follows: * Block - Block connections that have mismatch in content-type header and payload. * Log - Log connections that have mismatch in content-type header and payload. The mismatched content-type in HTTP request header will be logged for the request. * Stats - Generate statistics when there is mismatch in content-type header and payload.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			* None - Disable all actions for this security check. CLI users: To enable one or more actions, type "set appfw profile -inferContentTypeXMLPayloadAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -inferContentTypeXMLPayloadAction none". Please note "none" action cannot be used with any other action type. Possible values = block, log, stats, none
contenttypeaction	<String[]>	Read-write	One or more Content-type actions. Available settings function as follows: * Block - Block connections that violate this security check.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			* Learn - Use the learning engine to generate a list of exceptions to this security check. * Log - Log violations of this security check. * Stats - Generate statistics for this security check. * None - Disable all actions for this security check. CLI users: To enable one or more actions, type "set appfw profile -contentTypeaction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -contentTypeaction none". Possible values = none, block, learn, log, stats
inspectcontenttypes	<String[]>	Read-write	One or more InspectContentType lists.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			* application/x-www-form-urlencoded * multipart/form-data * text/x-gwt-rpc CLI users: To enable, type "set appfw profile -InspectContentTypes" followed by the content types to be inspected. Possible values = none, application/x-www-form-urlencoded, multipart/form-data, text/x-gwt-rpc, application/grpc, application/grpc-web+json, application/grpc-web-text
starturlclosure	<String>	Read-write	Toggle the state of Start URL Closure. Default value: OFF Possible values = ON, OFF
denyurlaction	<String[]>	Read-write	One or more Deny URL actions.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Available settings function as follows: * Block - Block connections that violate this security check. * Log - Log violations of this security check. * Stats - Generate statistics for this security check. * None - Disable all actions for this security check. NOTE: The Deny URL check takes precedence over the Start URL check. If you enable blocking for the Deny URL check, the application firewall blocks any URL that is explicitly blocked by a Deny URL, even if the same URL would otherwise be allowed by the Start URL check.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			CLI users: To enable one or more actions, type "set appfw profile -denyURLaction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -denyURLaction none". Possible values = none, block, log, stats
refererheadercheck	<String>	Read-write	Enable validation of Referer headers. Referer validation ensures that a web form that a user sends to your web site originally came from your web site, not an outside attacker. Although this parameter is part of the Start URL check, referer validation protects against cross-site request forgery

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			(CSRF) attacks, not Start URL attacks. Default value: OFF Possible values = OFF, if_present, AlwaysExceptStart URLs, AlwaysExceptFirstRequest
cookieconsistencyaction	<String[]>	Read-write	One or more Cookie Consistency actions. Available settings function as follows: * Block - Block connections that violate this security check. * Learn - Use the learning engine to generate a list of exceptions to this security check. * Log - Log violations of this security check. * Stats - Generate statistics for this security check. * None - Disable all actions for this security check.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			CLI users: To enable one or more actions, type "set appfw profile -cookieConsistency Action" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -cookieConsistency Action none". Default value: none Possible values = none, block, learn, log, stats
cookiehijackingaction	<String[]>	Read-write	One or more actions to prevent cookie hijacking. Available settings function as follows: * Block - Block connections that violate this security check. * Log - Log violations of this security check. * Stats - Generate statistics for this security check.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			* None - Disable all actions for this security check. NOTE: Cookie Hijacking feature is not supported for TLSv1.3 CLI users: To enable one or more actions, type "set appfw profile -cookieHijackingAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -cookieHijackingAction none". Default value: none Possible values = none, block, log, stats
cookietransforms	<String>	Read-write	Perform the specified type of cookie transformation. Available settings function as follows: * Encryption - Encrypt cookies.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			* Proxying - Mask contents of server cookies by sending proxy cookie to users. * Cookie flags - Flag cookies as HTTP only to prevent scripts on user's browser from accessing and possibly modifying them. CAUTION: Make sure that this parameter is set to ON if you are configuring any cookie transformations. If it is set to OFF, no cookie transformations are performed regardless of any other settings. Default value: OFF Possible values = ON, OFF
cookieencryption	<String>	Read-write	Type of cookie encryption. Available settings function as follows:

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			* None - Do not encrypt cookies. * Decrypt Only - Decrypt encrypted cookies, but do not encrypt cookies. * Encrypt Session Only - Encrypt session cookies, but not permanent cookies. * Encrypt All - Encrypt all cookies. Default value: none Possible values = none, decryptOnly, encryptSessionOnly , encryptAll
cookieproxying	<String>	Read-write	Cookie proxy setting. Available settings function as follows: * None - Do not proxy cookies. * Session Only - Proxy session cookies by using the Citrix ADC session ID, but do not proxy permanent cookies.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: none Possible values = none, sessionOnly
addcookieflags	<String>	Read-write	Add the specified flags to cookies. Available settings function as follows: * None - Do not add flags to cookies. * HTTP Only - Add the HTTP Only flag to cookies, which prevents scripts from accessing cookies. * Secure - Add Secure flag to cookies. * All - Add both HTTPOnly and Secure flags to cookies. Default value: none Possible values = none, httpOnly, secure, all
fieldconsistencyaction	<String[]>	Read-write	One or more Form Field Consistency actions. Available settings function as follows:

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			* Block - Block connections that violate this security check. * Learn - Use the learning engine to generate a list of exceptions to this security check. * Log - Log violations of this security check. * Stats - Generate statistics for this security check. * None - Disable all actions for this security check. CLI users: To enable one or more actions, type "set appfw profile -fieldConsistencyaction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -fieldConsistencyAction none". Default value: none

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = none, block, learn, log, stats
csrftagaction	<String[]>	Read-write	One or more Cross-Site Request Forgery (CSRF) Tagging actions. Available settings function as follows: * Block - Block connections that violate this security check. * Learn - Use the learning engine to generate a list of exceptions to this security check. * Log - Log violations of this security check. * Stats - Generate statistics for this security check. * None - Disable all actions for this security check. CLI users: To enable one or more actions, type "set appfw profile -CSRFTagAction" followed by the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			actions to be enabled. To turn off all actions, type "set appfw profile -CSRFTagAction none". Default value: none Possible values = none, block, learn, log, stats
crosssitescriptingaction	<String[]>	Read-write	One or more Cross-Site Scripting (XSS) actions. Available settings function as follows: * Block - Block connections that violate this security check. * Learn - Use the learning engine to generate a list of exceptions to this security check. * Log - Log violations of this security check. * Stats - Generate statistics for this security check.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			* None - Disable all actions for this security check. CLI users: To enable one or more actions, type "set appfw profile -crossSiteScriptingAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -crossSiteScriptingAction none". Possible values = none, block, learn, log, stats
crosssitescriptingtransformunsafehtml	<String>	Read-write	Transform cross-site scripts. This setting configures the application firewall to disable dangerous HTML instead of blocking the request. CAUTION: Make sure that this parameter is set to ON if you are configuring any cross-site scripting transformations. If it is set to OFF, no cross-site scripting transformations are

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			performed regardless of any other settings. Default value: OFF Possible values = ON, OFF
crosssitescriptingcheckcompleteurls	<String>	Read-write	Check complete URLs for cross-site scripts, instead of just the query portions of URLs. Default value: OFF Possible values = ON, OFF
sqlinjectionaction	<String[]>	Read-write	One or more HTML SQL Injection actions. Available settings function as follows: * Block - Block connections that violate this security check. * Learn - Use the learning engine to generate a list of exceptions to this security check. * Log - Log violations of this security check.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			* Stats - Generate statistics for this security check. * None - Disable all actions for this security check. CLI users: To enable one or more actions, type "set appfw profile -SQLInjectionAction " followed by the actions to be enabled. To turn off all actions, type "set appfw profile -SQLInjectionAction none". Possible values = none, block, learn, log, stats
cmdinjectionaction	<String[]>	Read-write	Command injection action. Available settings function as follows: * Block - Block connections that violate this security check. * Log - Log violations of this security check.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			* Stats - Generate statistics for this security check. * None - Disable all actions for this security check. CLI users: To enable one or more actions, type "set appfw profile -cmdInjectionAction " followed by the actions to be enabled. To turn off all actions, type "set appfw profile -cmdInjectionAction none". Default value: none Possible values = none, block, log, stats
cmdinjectiontype	<String>	Read-write	Available CMD injection types. -CMDSplChar : Checks for CMD Special Chars -CMDKeyword : Checks for CMD Keywords

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			-CMDSplCharANDKeyword : Checks for both and blocks if both are found -CMDSplCharORKeyword : Checks for both and blocks if anyone is found, -None : Disables checking using both CMD Special Char and Keyword. Default value: CMDSplCharANDKeyword Possible values = CMDSplChar, CMDKeyword, CMDSplCharORKeyword, CMDSplCharANDKeyword, None
sqlinjectiongrammar	<String>	Read-write	Check for SQL injection using SQL grammar. Default value: OFF Possible values = ON, OFF
cmdinjectiongrammar	<String>	Read-write	Check for CMD injection using CMD grammar.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: OFF Possible values = ON, OFF
fieldscan	<String>	Read-write	Check if formfield limit scan is ON or OFF. Default value: OFF Possible values = ON, OFF
fieldscanlimit	<Integer>	Read-write	Field scan limit value for HTML. Default value: 2048 Minimum value = 0 Maximum value = 16384
jsonfieldscan	<String>	Read-write	Check if JSON field limit scan is ON or OFF. Default value: OFF Possible values = ON, OFF
jsonfieldscanlimit	<Integer>	Read-write	Field scan limit value for JSON. Default value: 2048 Minimum value = 0 Maximum value = 16384

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
messagescan	<String>	Read-write	Check if HTML message limit scan is ON or OFF. Default value: OFF Possible values = ON, OFF
messagescanlimit	<Integer>	Read-write	Message scan limit value for HTML. Default value: 1000000 Minimum value = 0 Maximum value = 8000000
jsonmessagescan	<String>	Read-write	Check if JSON message limit scan is ON or OFF. Default value: OFF Possible values = ON, OFF
jsonmessagescanlimit	<Integer>	Read-write	Message scan limit value for JSON. Default value: 1000000 Minimum value = 0 Maximum value = 8000000
messagescanlimitcontenttypes	<String[]>	Read-write	Enable Message Scan Limit for following content types.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: NONE Possible values = FORM-DATA, JSON, NONE
sqlinjectiontransformspecialchars	<String>	Read-write	Transform injected SQL code. This setting configures the application firewall to disable SQL special strings instead of blocking the request. Since most SQL servers require a special string to activate an SQL keyword, in most cases a request that contains injected SQL code is safe if special strings are disabled. CAUTION: Make sure that this parameter is set to ON if you are configuring any SQL injection transformations. If it is set to OFF, no SQL injection transformations are performed regardless of any other settings.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: OFF Possible values = ON, OFF
sqlinjectiononlycheck fieldswithsqlchars	<String>	Read-write	Check only form fields that contain SQL special strings (characters) for injected SQL code. Most SQL servers require a special string to activate an SQL request, so SQL code without a special string is harmless to most SQL servers. Default value: ON Possible values = ON, OFF
sqlinjectiontype	<String>	Read-write	Available SQL injection types. -SQLSplChar : Checks for SQL Special Chars -SQLKeyword : Checks for SQL Keywords -SQLSplCharANDKeyword : Checks for both and blocks if both are found

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			-SQLSplCharORKeyword : Checks for both and blocks if anyone is found -None : Disables checking using both SQL Special Char and Keyword. Default value: SQLSplCharANDKeyword Possible values = SQLSplChar, SQLKeyword, SQLSplCharORKeyword, SQLSplCharANDKeyword, None
sqlinjectionchecksqlwildchars	<String>	Read-write	Check for form fields that contain SQL wild chars . Default value: OFF Possible values = ON, OFF
fieldformataction	<String[]>	Read-write	One or more Field Format actions. Available settings function as follows: * Block - Block connections that violate this security check.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			* Learn - Use the learning engine to generate a list of suggested web form fields and field format assignments. * Log - Log violations of this security check. * Stats - Generate statistics for this security check. * None - Disable all actions for this security check. CLI users: To enable one or more actions, type "set appfw profile -fieldFormatAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -fieldFormatAction none". Possible values = none, block, learn, log, stats
defaultfieldformattype	<String>	Read-write	Designate a default field type to be

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			applied to web form fields that do not have a field type explicitly assigned to them. Minimum length = 1
defaultfieldformatminlength	<Integer>	Read-write	Minimum length, in characters, for data entered into a field that is assigned the default field type. To disable the minimum and maximum length settings and allow data of any length to be entered into the field, set this parameter to zero (0). Default value: 0 Minimum value = 0 Maximum value = 2147483647
defaultfieldformatmaxlength	<Integer>	Read-write	Maximum length, in characters, for data entered into a field that is assigned the default field type. Default value: 65535 Minimum value = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum value = 2147483647
defaultfieldformatmaxoccurrences	<Integer>	Read-write	Maxiumum allowed occurrences of the form field name in a request. Default value: 65535 Minimum value = 0 Maximum value = 65535
bufferoverflowaction	<String[]>	Read-write	One or more Buffer Overflow actions. Available settings function as follows: * Block - Block connections that violate this security check. * Log - Log violations of this security check. * Stats - Generate statistics for this security check. * None - Disable all actions for this security check. CLI users: To enable one or more actions, type "set appfw profile

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			-bufferOverflowAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -bufferOverflowAction none". Possible values = none, block, log, stats
grpcaction	<String[]>	Read-write	gRPC validation. Possible values = none, block, log, stats
restaction	<String[]>	Read-write	rest validation. Possible values = none, block, log, stats
bufferoverflowmaxurllength	<Integer>	Read-write	Maximum length, in characters, for URLs on your protected web sites. Requests with longer URLs are blocked. Default value: 1024 Minimum value = 0 Maximum value = 65535
bufferoverflowmaxheaderlength	<Integer>	Read-write	Maximum length, in characters, for HTTP headers in requests

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			sent to your protected web sites. Requests with longer headers are blocked. Default value: 4096 Minimum value = 0 Maximum value = 65535
bufferoverflowmaxcookielength	<Integer>	Read-write	Maximum length, in characters, for cookies sent to your protected web sites. Requests with longer cookies are blocked. Default value: 4096 Minimum value = 0 Maximum value = 65535
bufferoverflowmaxquerylength	<Integer>	Read-write	Maximum length, in bytes, for query string sent to your protected web sites. Requests with longer query strings are blocked. Default value: 65535 Minimum value = 0 Maximum value = 65535
bufferoverflowmaxtotalheaderlength	<Integer>	Read-write	Maximum length, in bytes, for the total HTTP header length

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			in requests sent to your protected web sites. The minimum value of this and maxHeaderLen in httpProfile will be used. Requests with longer length are blocked. Default value: 65535 Minimum value = 0 Maximum value = 65535
creditcardaction	<String[]>	Read-write	One or more Credit Card actions. Available settings function as follows: * Block - Block connections that violate this security check. * Log - Log violations of this security check. * Stats - Generate statistics for this security check. * None - Disable all actions for this security check.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			CLI users: To enable one or more actions, type "set appfw profile -creditCardAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -creditCardAction none". Default value: none Possible values = none, block, learn, log, stats
creditcard	<String[]>	Read-write	Credit card types that the application firewall should protect. Default value: none Possible values = none, visa, mastercard, discover, amex, jcb, dinersclub
creditcardmaxallowed	<Integer>	Read-write	This parameter value is used by the block action. It represents the maximum number of credit card numbers that can appear on a web page served by your

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			protected web sites. Pages that contain more credit card numbers are blocked. Minimum value = 0 Maximum value = 255
creditcardxout	<String>	Read-write	Mask any credit card number detected in a response by replacing each digit, except the digits in the final group, with the letter "X.". Default value: OFF Possible values = ON, OFF
dosecurecreditcardlogging	<String>	Read-write	Setting this option logs credit card numbers in the response when the match is found. Default value: ON Possible values = ON, OFF
streaming	<String>	Read-write	Setting this option converts content-length form submission requests (requests with content-type "application/x-www-form-urlencoded" or "multipart/form-data")

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			to chunked requests when atleast one of the following protections : Signatures, SQL injection protection, XSS protection, form field consistency protection, starturl closure, CSRF tagging, JSON SQL, JSON XSS, JSON DOS is enabled. Please make sure that the backend server accepts chunked requests before enabling this option. Citrix recommends enabling this option for large request sizes(>20MB). Default value: OFF Possible values = ON, OFF
trace	<String>	Read-write	Toggle the state of trace. Default value: OFF Possible values = ON, OFF
requestcontenttype	<String>	Read-write	Default Content-Type header for requests. A Content-Type header can contain 0-255 letters,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			numbers, and the hyphen (-) and underscore (_) characters. Minimum length = 1 Maximum length = 255
responsecontenttype	<String>	Read-write	Default Content-Type header for responses. A Content-Type header can contain 0-255 letters, numbers, and the hyphen (-) and underscore (_) characters. Minimum length = 1 Maximum length = 255
jsonerrorobject	<String>	Read-write	Name to the imported JSON Error Object to be set on application firewall profile. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			name in double or single quotation marks \(for example, "my JSON error object" or 'my JSON error object'\). Minimum length = 1
apispec	<String>	Read-write	Name of the API Specification. Minimum length = 1
protofileobject	<String>	Read-write	Name of the imported proto file. Minimum length = 1
jsonerrorstatuscode	<Integer>	Read-write	Response status code associated with JSON error page. Non-empty JSON error object must be imported to the application firewall profile for the status code. Default value: 200 Minimum value = 1 Maximum value = 999
jsonerrorstatusmessage	<String>	Read-write	Response status message associated with JSON error page.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
jsondosaction	<String[]>	Read-write	One or more JSON Denial-of-Service (JsonDoS) actions. Available settings function as follows: * Block - Block connections that violate this security check. * Log - Log violations of this security check. * Stats - Generate statistics for this security check. * None - Disable all actions for this security check. CLI users: To enable one or more actions, type "set appfw profile -JSONDoSAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -JSONDoSAction none". Possible values = none, block, log, stats

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
jsonsqlinjectionaction	<String[]>	Read-write	One or more JSON SQL Injection actions. Available settings function as follows: * Block - Block connections that violate this security check. * Log - Log violations of this security check. * Stats - Generate statistics for this security check. * None - Disable all actions for this security check. CLI users: To enable one or more actions, type "set appfw profile -JSONSQLInjection Action" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -JSONSQLInjection Action none". Possible values = none, block, log, stats

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
jsonsqlinjectiontype	<String>	Read-write	Available SQL injection types. -SQLSplChar : Checks for SQL Special Chars -SQLKeyword : Checks for SQL Keywords -SQLSplCharANDKeyword : Checks for both and blocks if both are found -SQLSplCharORKeyword : Checks for both and blocks if anyone is found, -None : Disables checking using both SQL Special Char and Keyword. Default value: SQLSplCharANDKeyword Possible values = SQLSplChar, SQLKeyword, SQLSplCharORKeyword, SQLSplCharANDKeyword, None

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
jsonsqlinjectiongrammar	<String>	Read-write	Check for SQL injection using SQL grammar in JSON. Default value: OFF Possible values = ON, OFF
jsoncmdinjectionaction	<String[]>	Read-write	One or more JSON CMD Injection actions. Available settings function as follows: * Block - Block connections that violate this security check. * Log - Log violations of this security check. * Stats - Generate statistics for this security check. * None - Disable all actions for this security check. CLI users: To enable one or more actions, type "set appfw profile -JSONCMDInjectionAction" followed by the actions to be enabled. To turn off all actions, type "set

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			appfw profile -JSONCMDInjection Action none". Possible values = none, block, log, stats
jsoncmdinjectiontype	<String>	Read-write	Available CMD injection types. -CMDSplChar : Checks for CMD Special Chars -CMDKeyword : Checks for CMD Keywords -CMDSplCharANDKeyword : Checks for both and blocks if both are found -CMDSplCharORKeyword : Checks for both and blocks if anyone is found, -None : Disables checking using both SQL Special Char and Keyword. Default value: CMDSplCharANDKeyword Possible values = CMDSplChar,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			CMDKeyword, CMDSplCharORKeyword, CMDSplCharANDKeyword, None
jsoncmdinjectiongrammar	<String>	Read-write	Check for CMD injection using CMD grammar in JSON. Default value: OFF Possible values = ON, OFF
jsonxssaction	<String[]>	Read-write	One or more JSON Cross-Site Scripting actions. Available settings function as follows: * Block - Block connections that violate this security check. * Log - Log violations of this security check. * Stats - Generate statistics for this security check. * None - Disable all actions for this security check. CLI users: To enable one or more actions, type "set

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			appfw profile -JSONXssAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -JSONXssAction none". Possible values = none, block, log, stats
xmldosaction	<String[]>	Read-write	One or more XML Denial-of-Service (XDoS) actions. Available settings function as follows: * Block - Block connections that violate this security check. * Learn - Use the learning engine to generate a list of exceptions to this security check. * Log - Log violations of this security check. * Stats - Generate statistics for this security check.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			* None - Disable all actions for this security check. CLI users: To enable one or more actions, type "set appfw profile -XMLDoSAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -XMLDoSAction none". Possible values = none, block, learn, log, stats
xmlformataction	<String[]>	Read-write	One or more XML Format actions. Available settings function as follows: * Block - Block connections that violate this security check. * Log - Log violations of this security check. * Stats - Generate statistics for this security check.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			* None - Disable all actions for this security check. CLI users: To enable one or more actions, type "set appfw profile -XMLFormatAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -XMLFormatAction none". Possible values = none, block, log, stats
xmlsqlinjectionaction	<String[]>	Read-write	One or more XML SQL Injection actions. Available settings function as follows: * Block - Block connections that violate this security check. * Log - Log violations of this security check.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			* Stats - Generate statistics for this security check. * None - Disable all actions for this security check. CLI users: To enable one or more actions, type "set appfw profile -XMLSQLInjectionAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -XMLSQLInjectionAction none". Possible values = none, block, log, stats
xmlsqlinjectiononlycheckfieldswithsqlchars	<String>	Read-write	Check only form fields that contain SQL special characters, which most SQL servers require before accepting an SQL command, for injected SQL. Default value: ON Possible values = ON, OFF

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
xmlsqlinjectiontype	<String>	Read-write	Available SQL injection types. -SQLSplChar : Checks for SQL Special Chars -SQLKeyword : Checks for SQL Keywords -SQLSplCharANDKeyword : Checks for both and blocks if both are found -SQLSplCharORKeyword : Checks for both and blocks if anyone is found. Default value: SQLSplCharANDKeyword Possible values = SQLSplChar, SQLKeyword, SQLSplCharORKeyword, SQLSplCharANDKeyword, None
xmlsqlinjectioncheck sqlwildchars	<String>	Read-write	Check for form fields that contain SQL wild chars . Default value: OFF

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ON, OFF
xmlsqlinjectionparsecomments	<String>	Read-write	Parse comments in XML Data and exempt those sections of the request that are from the XML SQL Injection check. You must configure the type of comments that the application firewall is to detect and exempt from this security check. Available settings function as follows: * Check all - Check all content. * ANSI - Exempt content that is part of an ANSI (Mozilla-style) comment. * Nested - Exempt content that is part of a nested (Microsoft-style) comment. * ANSI Nested - Exempt content that is part of any type of comment. Default value: checkall

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = checkall, ansi, nested, ansinested
xmlxssaction	<String[]>	Read-write	One or more XML Cross-Site Scripting actions. Available settings function as follows: * Block - Block connections that violate this security check. * Log - Log violations of this security check. * Stats - Generate statistics for this security check. * None - Disable all actions for this security check. CLI users: To enable one or more actions, type "set appfw profile -XMLXSSAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			-XMLXSSAction none". Possible values = none, block, learn, log, stats
xmlwsiaction	<String[]>	Read-write	One or more Web Services Interoperability (WSI) actions. Available settings function as follows: * Block - Block connections that violate this security check. * Learn - Use the learning engine to generate a list of exceptions to this security check. * Log - Log violations of this security check. * Stats - Generate statistics for this security check. * None - Disable all actions for this security check. CLI users: To enable one or more actions, type "set

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			appfw profile -XMLWSIAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -XMLWSIAction none". Possible values = none, block, learn, log, stats
xmlattachmentaction	<String[]>	Read-write	One or more XML Attachment actions. Available settings function as follows: * Block - Block connections that violate this security check. * Learn - Use the learning engine to generate a list of exceptions to this security check. * Log - Log violations of this security check. * Stats - Generate statistics for this security check.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			* None - Disable all actions for this security check. CLI users: To enable one or more actions, type "set appfw profile -XMLAttachmentAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -XMLAttachmentAction none". Possible values = none, block, learn, log, stats
xmlvalidationaction	<String[]>	Read-write	One or more XML Validation actions. Available settings function as follows: * Block - Block connections that violate this security check. * Log - Log violations of this security check. * Stats - Generate statistics for this security check.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			* None - Disable all actions for this security check. CLI users: To enable one or more actions, type "set appfw profile -XMLValidationAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -XMLValidationAction none". Possible values = none, block, log, stats
xmlerrorobject	<String>	Read-write	Name to assign to the XML Error Object, which the application firewall displays when a user request is blocked. Must begin with a letter, number, or the underscore character \(_\), and must contain only letters, numbers, and the hyphen \(-\), period \(.\) pound \(#\), space \(\), at (@), equals \(=\), colon \(:\), and

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			underscore characters. Cannot be changed after the XML error object is added. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks \(for example, "my XML error object" or 'my XML error object'\). Minimum length = 1
xmlerrorstatuscode	<Integer>	Read-write	Response status code associated with XML error page. Non-empty XML error object must be imported to the application firewall profile for the status code. Default value: 200 Minimum value = 1 Maximum value = 999

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
xmlerrorstatusmessage	<String>	Read-write	Response status message associated with XML error page.
customsettings	<String>	Read-write	Object name for custom settings. This check is applicable to Profile Type: HTML, XML. . Minimum length = 1
signatures	<String>	Read-write	Object name for signatures. This check is applicable to Profile Type: HTML, XML. . Minimum length = 1
xmlsoapfaultaction	<String[]>	Read-write	One or more XML SOAP Fault Filtering actions. Available settings function as follows: * Block - Block connections that violate this security check. * Log - Log violations of this security check. * Stats - Generate statistics for this security check.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			* None - Disable all actions for this security check. * Remove - Remove all violations for this security check. CLI users: To enable one or more actions, type "set appfw profile -XMLSOAPFaultAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -XMLSOAPFaultAction none". Possible values = none, block, log, remove, stats
usehtmlerrorobject	<String>	Read-write	Send an imported HTML Error object to a user when a request is blocked, instead of redirecting the user to the designated Error URL. Default value: OFF Possible values = ON, OFF

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
errorurl	<String>	Read-write	URL that application firewall uses as the Error URL. Minimum length = 1
htmlerrorobject	<String>	Read-write	Name to assign to the HTML Error Object. Must begin with a letter, number, or the underscore character \(_\), and must contain only letters, numbers, and the hyphen \(-\), period \(.\) pound \(#\), space \(\), at (@), equals \(=\), colon \(:\), and underscore characters. Cannot be changed after the HTML error object is added. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks \(for example, "my HTML

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			error object" or 'my HTML error object'\). Minimum length = 1
htmlerrorstatuscode	<Integer>	Read-write	Response status code associated with HTML error page. Non-empty HTML error object must be imported to the application firewall profile for the status code. Default value: 200 Minimum value = 1 Maximum value = 999
htmlerrorstatusmessage	<String>	Read-write	Response status message associated with HTML error page.
logeverypolicyhit	<String>	Read-write	Log every profile match, regardless of security checks results. Default value: OFF Possible values = ON, OFF
stripcomments	<String>	Read-write	Strip HTML comments.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			This check is applicable to Profile Type: HTML. . Default value: OFF Possible values = ON, OFF
striphtmlcomments	<String>	Read-write	Strip HTML comments before forwarding a web page sent by a protected web site in response to a user request. Default value: none Possible values = none, all, exclude_script_tag
stripxmlcomments	<String>	Read-write	Strip XML comments before forwarding a web page sent by a protected web site in response to a user request. Default value: none Possible values = none, all
exemptclosureurlsfromsecuritychecks	<String>	Read-write	Exempt URLs that pass the Start URL closure check from SQL injection, cross-site script, field format and field consistency security

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			checks at locations other than headers. Default value: ON Possible values = ON, OFF
defaultcharset	<String>	Read-write	Default character set for protected web pages. Web pages sent by your protected web sites in response to user requests are assigned this character set if the page does not already specify a character set. The character sets supported by the application firewall are: * iso-8859-1 (English US) * big5 (Chinese Traditional) * gb2312 (Chinese Simplified) * sjis (Japanese Shift-JIS) * euc-jp (Japanese EUC-JP) * iso-8859-9 (Turkish)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			* utf-8 (Unicode) * euc-kr (Korean). Minimum length = 1 Maximum length = 31
clientipexpression	<String>	Read-write	Expression to get the client IP.
dynamiclearning	<String[]>	Read-write	One or more security checks. Available options are as follows: * SQLInjection - Enable dynamic learning for SQLInjection security check. * CrossSiteScripting - Enable dynamic learning for CrossSiteScripting security check. * fieldFormat - Enable dynamic learning for fieldFormat security check. * None - Disable security checks for all security checks.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			CLI users: To enable dynamic learning on one or more security checks, type "set appfw profile -dynamicLearning" followed by the security checks to be enabled. To turn off dynamic learning on all security checks, type "set appfw profile -dynamicLearning none". Possible values = none, SQLInjection, CrossSiteScripting, fieldFormat, startURL, cookieConsistency, fieldConsistency, CSRFtag, ContentType
postbodylimit	<Integer>	Read-write	Maximum allowed HTTP post body size, in bytes. Maximum supported value is 10GB. Citrix recommends enabling streaming option for large values of post body limit (>20MB).

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: 20000000
postbodylimitaction	<String[]>	Read-write	One or more Post Body Limit actions. Available settings function as follows: * Block - Block connections that violate this security check. Must always be set. * Log - Log violations of this security check. * Stats - Generate statistics for this security check. CLI users: To enable one or more actions, type "set appfw profile -PostBodyLimitAction block" followed by the other actions to be enabled. Possible values = block, log, stats
postbodylimitsignature	<Integer>	Read-write	Maximum allowed HTTP post body size for signature inspection for location HTTP_POST_BODY

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			in the signatures, in bytes. Note that the changes in value could impact CPU and latency profile. Default value: 2048
fileuploadmaxnum	<Integer>	Read-write	Maximum allowed number of file uploads per form-submission request. The maximum setting (65535) allows an unlimited number of uploads. Default value: 65535 Minimum value = 0 Maximum value = 65535
canonicalizehtmlresponse	<String>	Read-write	Perform HTML entity encoding for any special characters in responses sent by your protected web sites. Default value: ON Possible values = ON, OFF
enableformtagging	<String>	Read-write	Enable tagging of web form fields for use by the Form Field Consistency and CSRF Form Tagging checks.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: ON Possible values = ON, OFF
sessionlessfieldconsistency	<String>	Read-write	Perform sessionless Field Consistency Checks. Default value: OFF Possible values = OFF, ON, postOnly
sessionlessurlclosure	<String>	Read-write	Enable session less URL Closure Checks. This check is applicable to Profile Type: HTML. . Default value: OFF Possible values = ON, OFF
semicolonfieldseparator	<String>	Read-write	Allow ';' as a form field separator in URL queries and POST form bodies. . Default value: OFF Possible values = ON, OFF
excludefileuploadfromchecks	<String>	Read-write	Exclude uploaded files from Form checks. Default value: OFF

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ON, OFF
sqlinjectionparsecomments	<String>	Read-write	Parse HTML comments and exempt them from the HTML SQL Injection check. You must specify the type of comments that the application firewall is to detect and exempt from this security check. Available settings function as follows: * Check all - Check all content. * ANSI - Exempt content that is part of an ANSI (Mozilla-style) comment. * Nested - Exempt content that is part of a nested (Microsoft-style) comment. * ANSI Nested - Exempt content that is part of any type of comment. Possible values = checkall, ansi, nested, ansinested

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
invalidpercenthandling	<String>	Read-write	Configure the method that the application firewall uses to handle percent-encoded names and values. Available settings function as follows: * asp_mode - Microsoft ASP format. * secure_mode - Secure format. Default value: secure_mode Possible values = asp_mode, secure_mode
type	<String[]>	Read-write	Application firewall profile type, which controls which security checks and settings are applied to content that is filtered with the profile. Available settings function as follows: * HTML - HTML-based web sites. * XML - XML-based web sites and services.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			* JSON - JSON-based web sites and services. * HTML XML (Web 2.0) - Sites that contain both HTML and XML content, such as ATOM feeds, blogs, and RSS feeds. * HTML JSON - Sites that contain both HTML and JSON content. * XML JSON - Sites that contain both XML and JSON content. * HTML XML JSON - Sites that contain HTML, XML and JSON content. Default value: HTML Possible values = HTML, XML, JSON
checkrequestheaders	<String>	Read-write	Check request headers as well as web forms for injected SQL and cross-site scripts.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: OFF Possible values = ON, OFF
inspectquerycontenttypes	<String[]>	Read-write	Inspect request query as well as web forms for injected SQL and cross-site scripts for following content types. Possible values = HTML, XML, JSON, OTHER
optimizepartialreqs	<String>	Read-write	Optimize handle of HTTP partial requests i.e. those with range headers. Available settings are as follows: * ON - Partial requests by the client result in partial requests to the backend server in most cases. * OFF - Partial requests by the client are changed to full requests to the backend server. Default value: ON Possible values = ON, OFF

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
urldecoderequestcookies	<String>	Read-write	URL Decode request cookies before subjecting them to SQL and cross-site scripting checks. Default value: OFF Possible values = ON, OFF
comment	<String>	Read-write	Any comments about the purpose of profile, or other useful information about the profile.
percentdecoderecursively	<String>	Read-write	Configure whether the application firewall should use percentage recursive decoding. Default value: ON Possible values = ON, OFF
multipleheaderaction	<String[]>	Read-write	One or more multiple header actions. Available settings function as follows: * Block - Block connections that have multiple headers. * Log - Log connections that have multiple headers.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			* KeepLast - Keep only last header when multiple headers are present. Request headers inspected: * Accept-Encoding * Content-Encoding * Content-Range * Content-Type * Host * Range * Referer CLI users: To enable one or more actions, type "set appfw profile -multipleHeaderAction" followed by the actions to be enabled. Possible values = block, keepLast, log, none
rfcprofile	<String>	Read-write	Object name of the rfc profile. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
fileuploadtypesaction	<String[]>	Read-write	One or more file upload types actions. Available settings function as follows: * Block - Block connections that violate this security check. * Log - Log violations of this security check. * Stats - Generate statistics for this security check. * None - Disable all actions for this security check. CLI users: To enable one or more actions, type "set appfw profile -fileUploadTypeAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -fileUploadTypeAction none". Possible values = none, block, log, stats

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
verboseloglevel	<String>	Read-write	Detailed Logging Verbose Log Level. Default value: pattern Possible values = pattern, patternPayload, patternPayloadHeader
insertcookiesamesite attribute	<String>	Read-write	Configure whether application firewall should add samesite attribute for set-cookies. Default value: OFF Possible values = ON, OFF
cookiesamesiteattribute	<String>	Read-write	Cookie Samesite attribute added to support adding cookie SameSite attribute for all set-cookies including appfw session cookies. Default value will be "SameSite=Lax". Default value: LAX Possible values = None, LAX, STRICT
sqlinjectionruletype	<String>	Read-write	Specifies SQL Injection rule type: ALLOW/DENY. If ALLOW rule type is

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			configured then allow list rules are used, if DENY rule type is configured then deny rules are used. Default value: ALLOW Possible values = ALLOW, DENY
fakeaccountdetection	<String>	Read-write	Fake account detection flag : ON/OFF. If set to ON fake account detection in enabled on ADC, if set to OFF fake account detection is disabled. Default value: OFF Possible values = ON, OFF
geolocationlogging	<String>	Read-write	Enable Geo-Location Logging in CEF format logs for the profile. Possible values = ON, OFF
ceflogging	<String>	Read-write	Enable CEF format logs for the profile. Possible values = ON, OFF
blockkeywordaction	<String[]>	Read-write	Block Keyword action. Available settings function as follows:

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			* Block - Block connections that violate this security check. * Log - Log violations of this security check. * Stats - Generate statistics for this security check. * None - Disable all actions for this security check. CLI users: To enable one or more actions, type "set appfw profile -blockKeywordAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -blockKeywordAction none". Default value: none Possible values = none, block, log, stats
jsonblockkeywordaction	<String[]>	Read-write	JSON Block Keyword action.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Available settings function as follows: * Block - Block connections that violate this security check. * Log - Log violations of this security check. * Stats - Generate statistics for this security check. * None - Disable all actions for this security check. CLI users: To enable one or more actions, type "set appfw profile -JSONBlockKeywordAction" followed by the actions to be enabled. To turn off all actions, type "set appfw profile -JSONBlockKeywordAction none". Default value: none Possible values = none, block, log, stats

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
as_prof_bypass_list_enable	<String>	Read-write	Enable bypass list for the profile. Default value: OFF Possible values = ON, OFF
as_prof_deny_list_enable	<String>	Read-write	Enable deny list for the profile. Default value: OFF Possible values = ON, OFF
sessioncookiename	<String>	Read-write	Name of the session cookie that the application firewall uses to track user sessions. Must begin with a letter or number, and can consist of from 1 to 31 letters, numbers, and the hyphen (-) and underscore (_) symbols. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			"my cookie name" or 'my cookie name'). Minimum length = 1
archivename	<String>	Read-write	Source for tar archive. Minimum length = 1
relaxationrules	<Boolean>	Read-write	Import all appfw relaxation rules.
importprofilename	<String>	Read-write	Name of the profile which will be created/updated to associate the relaxation rules. Maximum length = 31
matchurlstring	<String>	Read-write	Match this action url in archived Relaxation Rules to replace. Maximum length = 2047
replaceurlstring	<String>	Read-write	Replace matched url string with this action url string while restoring Relaxation Rules. Maximum length = 2047
overwrite	<Boolean>	Read-write	Purge existing Relaxation Rules and replace during import.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
augment	<Boolean>	Read-write	Augment Relaxation Rules during import.
state	<String>	Read-only	Enabled. Possible values = ENABLED, DISABLED
learning	<String>	Read-only	Profile level learning option that overrides the protection level learning. Available settings are as follows: * ON - Honor all protection level learn settings. * OFF - Avoids learning for this profile for all protections ignoring protection level learn setting. Default value: ON Possible values = ON, OFF
csrftag	<String>	Read-only	The web form originating URL.
builtin	<Boolean>	Read-only	Indicates that a profile is a built-in entity.
_nextgenapiresource	<String>	Read-only	.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT
- RESTORE

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"appfwprofile":{

<b>"name":<String_value>,

</b>"defaults":<String_value>,

"starturlaction":<String[]_value>,

"infercontenttypexmlpayloadaction":<String[]_value>,

"contenttypeaction":<String[]_value>,

"inspectcontenttypes":<String[]_value>,

"starturlclosure":<String_value>,

"denyurlaction":<String[]_value>,

"refererheadercheck":<String_value>,

"cookieconsistencyaction":<String[]_value>,

"cookiehijackingaction":<String[]_value>,

"cookietransforms":<String_value>,

"cookieencryption":<String_value>,

"cookieproxying":<String_value>,
```

```
"addcookieflags":<String_value>,

"fieldconsistencyaction":<String[]_value>,

"csrftagaction":<String[]_value>,

"crosssitescriptingaction":<String[]_value>,

"crosssitescriptingtransformunsafehtml":<String_value>,

"crosssitescriptingcheckcompleteurls":<String_value>,

"sqlinjectionaction":<String[]_value>,

"cmdinjectionaction":<String[]_value>,

"cmdinjectiontype":<String_value>,

"sqlinjectiongrammar":<String_value>,

"cmdinjectiongrammar":<String_value>,

"fieldscan":<String_value>,

"fieldscanlimit":<Integer_value>,

"jsonfieldscan":<String_value>,

"jsonfieldscanlimit":<Integer_value>,

"messagescan":<String_value>,

"messagescanlimit":<Integer_value>,

"jsonmessagescan":<String_value>,

"jsonmessagescanlimit":<Integer_value>,

"messagescanlimitcontenttypes":<String[]_value>,

"sqlinjectiontransformspecialchars":<String_value>,

"sqlinjectiononlycheckfieldswithsqlchars":<String_value>,
```

```
"sqlinjectiontype":<String_value>,

"sqlinjectionchecksqlwildchars":<String_value>,

"fieldformataction":<String[]_value>,

"defaultfieldformattype":<String_value>,

"defaultfieldformatminlength":<Integer_value>,

"defaultfieldformatmaxlength":<Integer_value>,

"defaultfieldformatmaxoccurrences":<Integer_value>,

"bufferoverflowaction":<String[]_value>,

"grpcaction":<String[]_value>,

"restaction":<String[]_value>,

"bufferoverflowmaxurllength":<Integer_value>,

"bufferoverflowmaxheaderlength":<Integer_value>,

"bufferoverflowmaxcookielength":<Integer_value>,

"bufferoverflowmaxquerylength":<Integer_value>,

"bufferoverflowmaxtotalheaderlength":<Integer_value>,

"creditcardaction":<String[]_value>,

"creditcard":<String[]_value>,

"creditcardmaxallowed":<Integer_value>,

"creditcardxout":<String_value>,

"dosecurecreditcardlogging":<String_value>,

"streaming":<String_value>,

"trace":<String_value>,
```

```
"requestcontenttype":<String_value>,

"responsecontenttype":<String_value>,

"jsonerrorobject":<String_value>,

"apispec":<String_value>,

"protofileobject":<String_value>,

"jsonerrorstatuscode":<Integer_value>,

"jsonerrorstatusmessage":<String_value>,

"jsondosaction":<String[]_value>,

"jsonsqlinjectionaction":<String[]_value>,

"jsonsqlinjectiontype":<String_value>,

"jsonsqlinjectiongrammar":<String_value>,

"jsoncmdinjectionaction":<String[]_value>,

"jsoncmdinjectiontype":<String_value>,

"jsoncmdinjectiongrammar":<String_value>,

"jsonxssaction":<String[]_value>,

"xmldosaction":<String[]_value>,

"xmlformataction":<String[]_value>,

"xmlsqlinjectionaction":<String[]_value>,

"xmlsqlinjectiononlycheckfieldswithsqlchars":<String_value>,

"xmlsqlinjectiontype":<String_value>,

"xmlsqlinjectionchecksqlwildchars":<String_value>,

"xmlsqlinjectionparsecomments":<String_value>,
```

```
"xmlxssaction":<String[]_value>,

"xmlwsiaction":<String[]_value>,

"xmlattachmentaction":<String[]_value>,

"xmlvalidationaction":<String[]_value>,

"xmlerrorobject":<String_value>,

"xmlerrorstatuscode":<Integer_value>,

"xmlerrorstatusmessage":<String_value>,

"customsettings":<String_value>,

"signatures":<String_value>,

"xmlsoapfaultaction":<String[]_value>,

"usehtmlerrorobject":<String_value>,

"errorurl":<String_value>,

"htmlerrorobject":<String_value>,

"htmlerrorstatuscode":<Integer_value>,

"htmlerrorstatusmessage":<String_value>,

"logeverypolicyhit":<String_value>,

"stripcomments":<String_value>,

"striphtmlcomments":<String_value>,

"stripxmlcomments":<String_value>,

"exemptclosureurlsfromsecuritychecks":<String_value>,

"defaultcharset":<String_value>,

"clientipexpression":<String_value>,
```

```
"dynamiclearning":<String[]_value>,

"postbodylimit":<Integer_value>,

"postbodylimitaction":<String[]_value>,

"postbodylimitsignature":<Integer_value>,

"fileuploadmaxnum":<Integer_value>,

"canonicalizehtmlresponse":<String_value>,

"enableformtagging":<String_value>,

"sessionlessfieldconsistency":<String_value>,

"sessionlessurlclosure":<String_value>,

"semicolonfieldseparator":<String_value>,

"excludefileuploadfromchecks":<String_value>,

"sqlinjectionparsecomments":<String_value>,

"invalidpercenthandling":<String_value>,

"type":<String[]_value>,

"checkrequestheaders":<String_value>,

"inspectquerycontenttypes":<String[]_value>,

"optimizepartialreqs":<String_value>,

"urldecoderequestcookies":<String_value>,

"comment":<String_value>,

"percentdecoderecursively":<String_value>,

"multipleheaderaction":<String[]_value>,

"rfcprofile":<String_value>,
```

```
"fileuploadtypesaction":<String[]_value>,

"verboseloglevel":<String_value>,

"insertcookiesamesiteattribute":<String_value>,

"cookiesamesiteattribute":<String_value>,

"sqlinjectionruletype":<String_value>,

"fakeaccountdetection":<String_value>,

"geolocationlogging":<String_value>,

"ceflogging":<String_value>,

"blockkeywordaction":<String[]_value>,

"jsonblockkeywordaction":<String[]_value>,

"as_prof_bypass_list_enable":<String_value>,

"as_prof_deny_list_enable":<String_value>,

"sessioncookiename":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"appfwprofile":{

<b>"name":<String_value>,

</b>"starturlaction":<String[]_value>,

"infercontenttypexmlpayloadaction":<String[]_value>,

"contenttypeaction":<String[]_value>,

"inspectcontenttypes":<String[]_value>,

"starturlclosure":<String_value>,

"denyurlaction":<String[]_value>,

"refererheadercheck":<String_value>,

"cookieconsistencyaction":<String[]_value>,

"cookiehijackingaction":<String[]_value>,

"cookietransforms":<String_value>,

"cookieencryption":<String_value>,

"cookieproxying":<String_value>,

"addcookieflags":<String_value>,
```

```
"fieldconsistencyaction":<String[]_value>,

"csrftagaction":<String[]_value>,

"crosssitescriptingaction":<String[]_value>,

"crosssitescriptingtransformunsafehtml":<String_value>,

"crosssitescriptingcheckcompleteurls":<String_value>,

"sqlinjectionaction":<String[]_value>,

"cmdinjectionaction":<String[]_value>,

"cmdinjectiontype":<String_value>,

"sqlinjectiontransformspecialchars":<String_value>,

"sqlinjectiononlycheckfieldswithsqlchars":<String_value>,

"sqlinjectiontype":<String_value>,

"sqlinjectionchecksqlwildchars":<String_value>,

"sqlinjectiongrammar":<String_value>,

"cmdinjectiongrammar":<String_value>,

"fieldformataction":<String[]_value>,

"defaultfieldformattype":<String_value>,

"defaultfieldformatminlength":<Integer_value>,

"defaultfieldformatmaxlength":<Integer_value>,

"defaultfieldformatmaxoccurrences":<Integer_value>,

"fieldscan":<String_value>,

"fieldscanlimit":<Integer_value>,

"jsonfieldscan":<String_value>,
```

```
"jsonfieldscanlimit":<Integer_value>,

"messagescan":<String_value>,

"messagescanlimit":<Integer_value>,

"jsonmessagescan":<String_value>,

"jsonmessagescanlimit":<Integer_value>,

"messagescanlimitcontenttypes":<String[]_value>,

"bufferoverflowaction":<String[]_value>,

"grpcaction":<String[]_value>,

"restaction":<String[]_value>,

"bufferoverflowmaxurllength":<Integer_value>,

"bufferoverflowmaxheaderlength":<Integer_value>,

"bufferoverflowmaxcookielength":<Integer_value>,

"bufferoverflowmaxquerylength":<Integer_value>,

"bufferoverflowmaxtotalheaderlength":<Integer_value>,

"creditcardaction":<String[]_value>,

"creditcard":<String[]_value>,

"creditcardmaxallowed":<Integer_value>,

"creditcardxout":<String_value>,

"dosecurecreditcardlogging":<String_value>,

"streaming":<String_value>,

"trace":<String_value>,

"requestcontenttype":<String_value>,
```

```
"responsecontenttype":<String_value>,

"jsonerrorobject":<String_value>,

"jsonerrorstatuscode":<Integer_value>,

"jsonerrorstatusmessage":<String_value>,

"apispec":<String_value>,

"protofileobject":<String_value>,

"jsondosaction":<String[]_value>,

"jsonsqlinjectionaction":<String[]_value>,

"jsonsqlinjectiontype":<String_value>,

"jsonsqlinjectiongrammar":<String_value>,

"jsoncmdinjectionaction":<String[]_value>,

"jsoncmdinjectiontype":<String_value>,

"jsoncmdinjectiongrammar":<String_value>,

"jsonxssaction":<String[]_value>,

"xmldosaction":<String[]_value>,

"xmlformataction":<String[]_value>,

"xmlsqlinjectionaction":<String[]_value>,

"xmlsqlinjectiononlycheckfieldswithsqlchars":<String_value>,

"xmlsqlinjectiontype":<String_value>,

"xmlsqlinjectionchecksqlwildchars":<String_value>,

"xmlsqlinjectionparsecomments":<String_value>,

"xmlxssaction":<String[]_value>,
```

```
"xmlwsiaction":<String[]_value>,

"xmlattachmentaction":<String[]_value>,

"xmlvalidationaction":<String[]_value>,

"xmlerrorobject":<String_value>,

"xmlerrorstatuscode":<Integer_value>,

"xmlerrorstatusmessage":<String_value>,

"customsettings":<String_value>,

"signatures":<String_value>,

"xmlsoapfaultaction":<String[]_value>,

"usehtmlerrorobject":<String_value>,

"errorurl":<String_value>,

"htmlerrorobject":<String_value>,

"htmlerrorstatuscode":<Integer_value>,

"htmlerrorstatusmessage":<String_value>,

"logeverypolicyhit":<String_value>,

"stripcomments":<String_value>,

"striphtmlcomments":<String_value>,

"stripxmlcomments":<String_value>,

"clientipexpression":<String_value>,

"dynamiclearning":<String[]_value>,

"exemptclosureurlsfromsecuritychecks":<String_value>,

"defaultcharset":<String_value>,
```

```
"postbodylimit":<Integer_value>,

"postbodylimitaction":<String[]_value>,

"postbodylimitsignature":<Integer_value>,

"fileuploadmaxnum":<Integer_value>,

"canonicalizehtmlresponse":<String_value>,

"enableformtagging":<String_value>,

"sessionlessfieldconsistency":<String_value>,

"sessionlessurlclosure":<String_value>,

"semicolonfieldseparator":<String_value>,

"excludefileuploadfromchecks":<String_value>,

"sqlinjectionparsecomments":<String_value>,

"invalidpercenthandling":<String_value>,

"type":<String[]_value>,

"checkrequestheaders":<String_value>,

"inspectquerycontenttypes":<String[]_value>,

"optimizepartialreqs":<String_value>,

"urldecoderequestcookies":<String_value>,

"comment":<String_value>,

"percentdecoderecursively":<String_value>,

"multipleheaderaction":<String[]_value>,

"rfcprofile":<String_value>,

"fileuploadtypesaction":<String[]_value>,
```

```
"verboseloglevel":<String_value>,

"insertcookiesamesiteattribute":<String_value>,

"cookiesamesiteattribute":<String_value>,

"sqlinjectionruletype":<String_value>,

"fakeaccountdetection":<String_value>,

"geolocationlogging":<String_value>,

"ceflogging":<String_value>,

"blockkeywordaction":<String[]_value>,

"jsonblockkeywordaction":<String[]_value>,

"as_prof_bypass_list_enable":<String_value>,

"as_prof_deny_list_enable":<String_value>,

"sessioncookiename":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"appfwprofile":{

<b>"name":<String_value>,

</b>"starturlaction":true,

"infercontenttypexmlpayloadaction":true,

"contenttypeaction":true,

"inspectcontenttypes":true,

"starturlclosure":true,

"denyurlaction":true,

"refererheadercheck":true,

"cookieconsistencyaction":true,

"cookiehijackingaction":true,

"cookietransforms":true,

"cookieencryption":true,

"cookieproxying":true,

"addcookieflags":true,

"fieldconsistencyaction":true,

"csrftagaction":true,

"crosssitescriptingaction":true,

"crosssitescriptingtransformunsafehtml":true,

"crosssitescriptingcheckcompleteurls":true,

"sqlinjectionaction":true,

"cmdinjectionaction":true,
```

```
"cmdinjectiontype":true,

"sqlinjectiontransformspecialchars":true,

"sqlinjectiononlycheckfieldswithsqlchars":true,

"sqlinjectiontype":true,

"sqlinjectionchecksqlwildchars":true,

"sqlinjectiongrammar":true,

"cmdinjectiongrammar":true,

"fieldformataction":true,

"defaultfieldformattype":true,

"defaultfieldformatminlength":true,

"defaultfieldformatmaxlength":true,

"defaultfieldformatmaxoccurrences":true,

"fieldscan":true,

"fieldscanlimit":true,

"jsonfieldscan":true,

"jsonfieldscanlimit":true,

"messagescan":true,

"messagescanlimit":true,

"jsonmessagescan":true,

"jsonmessagescanlimit":true,

"messagescanlimitcontenttypes":true,

"bufferoverflowaction":true,
```

```
"grpcaction":true,

"restaction":true,

"bufferoverflowmaxurllength":true,

"bufferoverflowmaxheaderlength":true,

"bufferoverflowmaxcookielength":true,

"bufferoverflowmaxquerylength":true,

"bufferoverflowmaxtotalheaderlength":true,

"creditcardaction":true,

"creditcard":true,

"creditcardmaxallowed":true,

"creditcardxout":true,

"dosecurecreditcardlogging":true,

"streaming":true,

"trace":true,

"requestcontenttype":true,

"responsecontenttype":true,

"jsonerrorobject":true,

"jsonerrorstatuscode":true,

"jsonerrorstatusmessage":true,

"apispec":true,

"protofileobject":true,

"jsondosaction":true,
```

```
"jsonsqlinjectionaction":true,

"jsonsqlinjectiontype":true,

"jsonsqlinjectiongrammar":true,

"jsoncmdinjectionaction":true,

"jsoncmdinjectiontype":true,

"jsoncmdinjectiongrammar":true,

"jsonxssaction":true,

"xmldosaction":true,

"xmlformataction":true,

"xmlsqlinjectionaction":true,

"xmlsqlinjectiononlycheckfieldswithsqlchars":true,

"xmlsqlinjectiontype":true,

"xmlsqlinjectionchecksqlwildchars":true,

"xmlsqlinjectionparsecomments":true,

"xmlxssaction":true,

"xmlwsiaction":true,

"xmlattachmentaction":true,

"xmlvalidationaction":true,

"xmlerrorobject":true,

"xmlerrorstatuscode":true,

"xmlerrorstatusmessage":true,

"customsettings":true,
```

```
"signatures":true,

"xmlsoapfaultaction":true,

"usehtmlerrorobject":true,

"errorurl":true,

"htmlerrorobject":true,

"htmlerrorstatuscode":true,

"htmlerrorstatusmessage":true,

"logeverypolicyhit":true,

"stripcomments":true,

"striphtmlcomments":true,

"stripxmlcomments":true,

"clientipexpression":true,

"dynamiclearning":true,

"exemptclosureurlsfromsecuritychecks":true,

"defaultcharset":true,

"postbodylimit":true,

"postbodylimitaction":true,

"postbodylimitsignature":true,

"fileuploadmaxnum":true,

"canonicalizehtmlresponse":true,

"enableformtagging":true,

"sessionlessfieldconsistency":true,
```

```
"sessionlessurlclosure":true,

"semicolonfieldseparator":true,

"excludefileuploadfromchecks":true,

"sqlinjectionparsecomments":true,

"invalidpercenthandling":true,

"type":true,

"checkrequestheaders":true,

"inspectquerycontenttypes":true,

"optimizepartialreqs":true,

"urldecoderequestcookies":true,

"comment":true,

"percentdecoderecursively":true,

"multipleheaderaction":true,

"rfcprofile":true,

"fileuploadtypesaction":true,

"verboseloglevel":true,

"insertcookiesamesiteattribute":true,

"cookiesamesiteattribute":true,

"sqlinjectionruletype":true,

"fakeaccountdetection":true,

"geolocationlogging":true,

"ceflogging":true,
```

```
"blockkeywordaction":true,

"jsonblockkeywordaction":true,

"as_prof_bypass_list_enable":true,

"as_prof_deny_list_enable":true,

"sessioncookiename":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

RESTORE

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile? **action=restore HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"appfwprofile":{

<b>"archivename":<String_value>,

</b>"relaxationrules":<Boolean_value>,

"importprofilename":<String_value>,

"matchurlstring":<String_value>,

"replaceurlstring":<String_value>,
```

```
"overwrite":<Boolean_value>,

"augment":<Boolean_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of appfwprofile resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile? **view=summary**

Use this query-parameter to get the summary output of appfwprofile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile? **pagesize=#no;pageno=#no**

Use this query-parameter to get the appfwprofile resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "appfwprofile": [ {

"name":<String_value>,

"type":<String[]_value>,

"state":<String_value>,

"defaults":<String_value>,

"usehtmlerrorobject":<String_value>,

"errorurl":<String_value>,

"htmlerrorobject":<String_value>,

"htmlerrorstatuscode":<Integer_value>,

"htmlerrorstatusmessage":<String_value>,

"logeverypolicyhit":<String_value>,

"stripcomments":<String_value>,

"striphtmlcomments":<String_value>,

"stripxmlcomments":<String_value>,

"defaultcharset":<String_value>,

"postbodylimit":<Integer_value>,

"postbodylimitaction":<String[]_value>,
```

```
"clientipexpression":<String_value>,

"dynamiclearning":<String[]_value>,

"postbodylimitsignature":<Integer_value>,

"learning":<String_value>,

"fileuploadmaxnum":<Integer_value>,

"canonicalizehtmlresponse":<String_value>,

"enableformtagging":<String_value>,

"sessionlessfieldconsistency":<String_value>,

"sessionlessurlclosure":<String_value>,

"semicolonfieldseparator":<String_value>,

"excludefileuploadfromchecks":<String_value>,

"sqlinjectionparsecomments":<String_value>,

"checkrequestheaders":<String_value>,

"inspectquerycontenttypes":<String[]_value>,

"optimizepartialreqs":<String_value>,

"urldecoderequestcookies":<String_value>,

"starturlaction":<String[]_value>,

"infercontenttypexmlpayloadaction":<String[]_value>,

"contenttypeaction":<String[]_value>,

"inspectcontenttypes":<String[]_value>,

"starturlclosure":<String_value>,

"denyurlaction":<String[]_value>,
```

```
"refererheadercheck":<String_value>,

"csrftagaction":<String[]_value>,

"csrftag":<String_value>,

"crosssitescriptingaction":<String[]_value>,

"crosssitescriptingtransformunsafehtml":<String_value>,

"crosssitescriptingcheckcompleteurls":<String_value>,

"exemptclosureurlsfromsecuritychecks":<String_value>,

"sqlinjectionaction":<String[]_value>,

"cmdinjectionaction":<String[]_value>,

"sqlinjectiontransformspecialchars":<String_value>,

"sqlinjectiononlycheckfieldswithsqlchars":<String_value>,

"sqlinjectiontype":<String_value>,

"cmdinjectiontype":<String_value>,

"sqlinjectiongrammar":<String_value>,

"cmdinjectiongrammar":<String_value>,

"fieldscan":<String_value>,

"fieldscanlimit":<Integer_value>,

"jsonfieldscan":<String_value>,

"jsonfieldscanlimit":<Integer_value>,

"messagescan":<String_value>,

"messagescanlimit":<Integer_value>,

"jsonmessagescan":<String_value>,
```

```
"jsonmessagescanlimit":<Integer_value>,

"messagescanlimitcontenttypes":<String[]_value>,

"sqlinjectionchecksqlwildchars":<String_value>,

"invalidpercenthandling":<String_value>,

"fieldconsistencyaction":<String[]_value>,

"cookieconsistencyaction":<String[]_value>,

"cookiehijackingaction":<String[]_value>,

"cookietransforms":<String_value>,

"cookieencryption":<String_value>,

"cookieproxying":<String_value>,

"addcookieflags":<String_value>,

"bufferoverflowaction":<String[]_value>,

"grpcaction":<String[]_value>,

"restaction":<String[]_value>,

"bufferoverflowmaxurllength":<Integer_value>,

"bufferoverflowmaxheaderlength":<Integer_value>,

"bufferoverflowmaxcookielength":<Integer_value>,

"bufferoverflowmaxquerylength":<Integer_value>,

"bufferoverflowmaxtotalheaderlength":<Integer_value>,

"fieldformataction":<String[]_value>,

"defaultfieldformattype":<String_value>,

"defaultfieldformatminlength":<Integer_value>,
```

```
"defaultfieldformatmaxlength":<Integer_value>,

"defaultfieldformatmaxoccurrences":<Integer_value>,

"creditcardaction":<String[]_value>,

"creditcard":<String[]_value>,

"creditcardmaxallowed":<Integer_value>,

"creditcardxout":<String_value>,

"dosecurecreditcardlogging":<String_value>,

"streaming":<String_value>,

"trace":<String_value>,

"requestcontenttype":<String_value>,

"responsecontenttype":<String_value>,

"xmlerrorobject":<String_value>,

"xmlerrorstatuscode":<Integer_value>,

"xmlerrorstatusmessage":<String_value>,

"signatures":<String_value>,

"xmlformataction":<String[]_value>,

"xmldosaction":<String[]_value>,

"xmlsqlinjectionaction":<String[]_value>,

"xmlsqlinjectiononlycheckfieldswithsqlchars":<String_value>,

"xmlsqlinjectiontype":<String_value>,

"xmlsqlinjectionchecksqlwildchars":<String_value>,

"xmlsqlinjectionparsecomments":<String_value>,
```

```
"xmlxssaction":<String[]_value>,

"xmlwsiaction":<String[]_value>,

"xmlattachmentaction":<String[]_value>,

"xmlvalidationaction":<String[]_value>,

"xmlsoapfaultaction":<String[]_value>,

"builtin":<Boolean_value>,

"comment":<String_value>,

"percentdecoderecursively":<String_value>,

"multipleheaderaction":<String[]_value>,

"rfcprofile":<String_value>,

"apispec":<String_value>,

"protofileobject":<String_value>,

"jsonerrorobject":<String_value>,

"jsonerrorstatuscode":<Integer_value>,

"jsonerrorstatusmessage":<String_value>,

"jsondosaction":<String[]_value>,

"jsonsqlinjectionaction":<String[]_value>,

"jsonsqlinjectiontype":<String_value>,

"jsonsqlinjectiongrammar":<String_value>,

"jsoncmdinjectionaction":<String[]_value>,

"jsoncmdinjectiontype":<String_value>,

"jsoncmdinjectiongrammar":<String_value>,
```

```
"jsonxssaction":<String[]_value>,

"fileuploadtypesaction":<String[]_value>,

"verboseloglevel":<String_value>,

"insertcookiesamesiteattribute":<String_value>,

"cookiesamesiteattribute":<String_value>,

"sqlinjectionruletype":<String_value>,

"fakeaccountdetection":<String_value>,

"geolocationlogging":<String_value>,

"ceflogging":<String_value>,

"blockkeywordaction":<String[]_value>,

"jsonblockkeywordaction":<String[]_value>,

"as_prof_bypass_list_enable":<String_value>,

"as_prof_deny_list_enable":<String_value>,

"sessioncookiename":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of appfwprofile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwprofile": [ {

"name":<String_value>,

"type":<String[]_value>,

"state":<String_value>,

"defaults":<String_value>,

"usehtmlerrorobject":<String_value>,

"errorurl":<String_value>,

"htmlerrorobject":<String_value>,

"htmlerrorstatuscode":<Integer_value>,

"htmlerrorstatusmessage":<String_value>,
```

```
"logeverypolicyhit":<String_value>,

"stripcomments":<String_value>,

"striphtmlcomments":<String_value>,

"stripxmlcomments":<String_value>,

"defaultcharset":<String_value>,

"postbodylimit":<Integer_value>,

"postbodylimitaction":<String[]_value>,

"clientipexpression":<String_value>,

"dynamiclearning":<String[]_value>,

"postbodylimitsignature":<Integer_value>,

"learning":<String_value>,

"fileuploadmaxnum":<Integer_value>,

"canonicalizehtmlresponse":<String_value>,

"enableformtagging":<String_value>,

"sessionlessfieldconsistency":<String_value>,

"sessionlessurlclosure":<String_value>,

"semicolonfieldseparator":<String_value>,

"excludefileuploadfromchecks":<String_value>,

"sqlinjectionparsecomments":<String_value>,

"checkrequestheaders":<String_value>,

"inspectquerycontenttypes":<String[]_value>,

"optimizepartialreqs":<String_value>,
```

```
"urldecoderequestcookies":<String_value>,

"starturlaction":<String[]_value>,

"infercontenttypexmlpayloadaction":<String[]_value>,

"contenttypeaction":<String[]_value>,

"inspectcontenttypes":<String[]_value>,

"starturlclosure":<String_value>,

"denyurlaction":<String[]_value>,

"refererheadercheck":<String_value>,

"csrftagaction":<String[]_value>,

"csrftag":<String_value>,

"crosssitescriptingaction":<String[]_value>,

"crosssitescriptingtransformunsafehtml":<String_value>,

"crosssitescriptingcheckcompleteurls":<String_value>,

"exemptclosureurlsfromsecuritychecks":<String_value>,

"sqlinjectionaction":<String[]_value>,

"cmdinjectionaction":<String[]_value>,

"sqlinjectiontransformspecialchars":<String_value>,

"sqlinjectiononlycheckfieldswithsqlchars":<String_value>,

"sqlinjectiontype":<String_value>,

"cmdinjectiontype":<String_value>,

"sqlinjectiongrammar":<String_value>,

"cmdinjectiongrammar":<String_value>,
```

```
"fieldscan":<String_value>,

"fieldscanlimit":<Integer_value>,

"jsonfieldscan":<String_value>,

"jsonfieldscanlimit":<Integer_value>,

"messagescan":<String_value>,

"messagescanlimit":<Integer_value>,

"jsonmessagescan":<String_value>,

"jsonmessagescanlimit":<Integer_value>,

"messagescanlimitcontenttypes":<String[]_value>,

"sqlinjectionchecksqlwildchars":<String_value>,

"invalidpercenthandling":<String_value>,

"fieldconsistencyaction":<String[]_value>,

"cookieconsistencyaction":<String[]_value>,

"cookiehijackingaction":<String[]_value>,

"cookietransforms":<String_value>,

"cookieencryption":<String_value>,

"cookieproxying":<String_value>,

"addcookieflags":<String_value>,

"bufferoverflowaction":<String[]_value>,

"grpcaction":<String[]_value>,

"restaction":<String[]_value>,

"bufferoverflowmaxurllength":<Integer_value>,
```

```
"bufferoverflowmaxheaderlength":<Integer_value>,

"bufferoverflowmaxcookielength":<Integer_value>,

"bufferoverflowmaxquerylength":<Integer_value>,

"bufferoverflowmaxtotalheaderlength":<Integer_value>,

"fieldformataction":<String[]_value>,

"defaultfieldformattype":<String_value>,

"defaultfieldformatminlength":<Integer_value>,

"defaultfieldformatmaxlength":<Integer_value>,

"defaultfieldformatmaxoccurrences":<Integer_value>,

"creditcardaction":<String[]_value>,

"creditcard":<String[]_value>,

"creditcardmaxallowed":<Integer_value>,

"creditcardxout":<String_value>,

"dosecurecreditcardlogging":<String_value>,

"streaming":<String_value>,

"trace":<String_value>,

"requestcontenttype":<String_value>,

"responsecontenttype":<String_value>,

"xmlerrorobject":<String_value>,

"xmlerrorstatuscode":<Integer_value>,

"xmlerrorstatusmessage":<String_value>,

"signatures":<String_value>,
```

```
"xmlformataction":<String[]_value>,

"xmldosaction":<String[]_value>,

"xmlsqlinjectionaction":<String[]_value>,

"xmlsqlinjectiononlycheckfieldswithsqlchars":<String_value>,

"xmlsqlinjectiontype":<String_value>,

"xmlsqlinjectionchecksqlwildchars":<String_value>,

"xmlsqlinjectionparsecomments":<String_value>,

"xmlxssaction":<String[]_value>,

"xmlwsiaction":<String[]_value>,

"xmlattachmentaction":<String[]_value>,

"xmlvalidationaction":<String[]_value>,

"xmlsoapfaultaction":<String[]_value>,

"builtin":<Boolean_value>,

"comment":<String_value>,

"percentdecoderecursively":<String_value>,

"multipleheaderaction":<String[]_value>,

"rfcprofile":<String_value>,

"apispec":<String_value>,

"protofileobject":<String_value>,

"jsonerrorobject":<String_value>,

"jsonerrorstatuscode":<Integer_value>,

"jsonerrorstatusmessage":<String_value>,
```

```
"jsondosaction":<String[]_value>,

"jsonsqlinjectionaction":<String[]_value>,

"jsonsqlinjectiontype":<String_value>,

"jsonsqlinjectiongrammar":<String_value>,

"jsoncmdinjectionaction":<String[]_value>,

"jsoncmdinjectiontype":<String_value>,

"jsoncmdinjectiongrammar":<String_value>,

"jsonxssaction":<String[]_value>,

"fileuploadtypesaction":<String[]_value>,

"verboseloglevel":<String_value>,

"insertcookiesamesiteattribute":<String_value>,

"cookiesamesiteattribute":<String_value>,

"sqlinjectionruletype":<String_value>,

"fakeaccountdetection":<String_value>,

"geolocationlogging":<String_value>,

"ceflogging":<String_value>,

"blockkeywordaction":<String[]_value>,

"jsonblockkeywordaction":<String[]_value>,

"as_prof_bypass_list_enable":<String_value>,

"as_prof_deny_list_enable":<String_value>,

"sessioncookiename":<String_value>,

"_nextgenapiresource":<String_value>
```

```
}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "appfwprofile": [ { "__count": "#no"} ] }
```

appfwprofile_appfwconfidfield_binding

Binding object showing the appfwconfidfield that can be bound to appfwprofile.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
alertonly	<String>	Read-write	Send SNMP alert?. Possible values = ON, OFF
ruletype	<String>	Read-write	Specifies rule type of binding.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ALLOW, DENY
isautodeployed	<String>	Read-write	Is the rule auto deployed by dynamic profile ?. Possible values = AUTODEPLOYED, NOTAUTODEPLOYED
name	<String>	Read-write	Name of the profile to which to bind an exemption or rule. Minimum length = 1
resourceid	<String>	Read-write	A "id" that identifies the rule.
cffield_url	<String>	Read-write	URL of the web page that contains the web form. Minimum length = 1
confidfield	<String>	Read-write	Name of the form field to designate as confidential. Minimum length = 1
isregex_cffield	<String>	Read-write	Is Fake Account Detection field name regular expression?. Possible values = REGEX, NOTREGEX
state	<String>	Read-write	Enabled.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ENABLED, DISABLED
comment	<String>	Read-write	Any comments about the purpose of profile, or other useful information about the profile.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/appfwprofile_appfwconfidfield_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"appfwprofile_appfwconfidfield_binding":{

<b>"name":<String_value>,

</b>"comment":<String_value>,

"state":<String_value>,

"isautodeployed":<String_value>,

"resourceid":<String_value>,

"confidfield":<String_value>,

"cffield_url":<String_value>,

"isregex_cffield":<String_value>,

"ruletype":<String_value>
```

```
}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_appfwconfidfield_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ appfwprofile_appfwconfidfield_binding/ name_value<String> ? **args=confidfield: <String_value> ,cffield_url: <String_value> ,ruletype: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_appfwconfidfield_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ appfwprofile_appfwconfidfield_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of appfwprofile_appfwconfidfield_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_appfwconfidfield_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the appfwprofile_appfwconfidfield_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwprofile_appfwconfidfield_binding": [ {

"alertonly":<String_value>,

"ruletype":<String_value>,

"isautodeployed":<String_value>,

"name":<String_value>,

"resourceid":<String_value>,

"cffield_url":<String_value>,

"confidfield":<String_value>,

"isregex_cffield":<String_value>,

"state":<String_value>,

"comment":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_appfwconfidfield_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_appfwconfidfield_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwprofile_appfwconfidfield_binding": [ {

"alertonly":<String_value>,

"ruletype":<String_value>,

"isautodeployed":<String_value>,

"name":<String_value>,

"resourceid":<String_value>,

"cffield_url":<String_value>,

"confidfield":<String_value>,

"isregex_cffield":<String_value>,

"state":<String_value>,
```

```
"comment":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_appfwconfidfield_binding/name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"appfwprofile_appfwconfidfield_binding": [ { "__count": "#no"} ] }
```

appfwprofile_binding

Binding object which returns the resources bound to appfwprofile.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the application firewall profile. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
appfwprofile_bypasslist_binding	<appfwprofile_bypasslist_binding[]>	Read-only	bypasslist that can be bound to appfwprofile.
appfwprofile_xmlxss_binding	<appfwprofile_xmlxss_binding[]>	Read-only	xmlxss that can be bound to appfwprofile.
appfwprofile_jsondosurl_binding	<appfwprofile_jsondosurl_binding[]>	Read-only	jsondosurl that can be bound to appfwprofile.
appfwprofile_jsonblockkeyword_binding	<appfwprofile_jsonblockkeyword_binding[]>	Read-only	jsonblockkeyword that can be bound to appfwprofile.
appfwprofile_contenttype_binding	<appfwprofile_contenttype_binding[]>	Read-only	contenttype that can be bound to appfwprofile.
appfwprofile_starturl_binding	<appfwprofile_starturl_binding[]>	Read-only	starturl that can be bound to appfwprofile.
appfwprofile_logexpression_binding	<appfwprofile_logexpression_binding[]>	Read-only	logexpression that can be bound to appfwprofile.
appfwprofile_xmlsqlinjection_binding	<appfwprofile_xmlsqlinjection_binding[]>	Read-only	xmlsqlinjection that can be bound to appfwprofile.
appfwprofile_grpcvalidation_binding	<appfwprofile_grpcvalidation_binding[]>	Read-only	grpcvalidation that can be bound to appfwprofile.
appfwprofile_jsonsqlurl_binding	<appfwprofile_jsonsqlurl_binding[]>	Read-only	jsonsqlurl that can be bound to appfwprofile.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
appfwprofile_jsonxssurl_binding	<appfwprofile_jsonxssurl_binding[]>	Read-only	jsonxssurl that can be bound to appfwprofile.
appfwprofile_jsoncmdurl_binding	<appfwprofile_jsoncmdurl_binding[]>	Read-only	jsoncmdurl that can be bound to appfwprofile.
appfwprofile_cookieconsistency_binding	<appfwprofile_cookieconsistency_binding[]>	Read-only	cookieconsistency that can be bound to appfwprofile.
appfwprofile_excluderescontenttype_binding	<appfwprofile_excluderescontenttype_binding[]>	Read-only	excluderescontenttype that can be bound to appfwprofile.
appfwprofile_sqlinjection_binding	<appfwprofile_sqlinjection_binding[]>	Read-only	sqlinjection that can be bound to appfwprofile.
appfwprofile_blockkeyword_binding	<appfwprofile_blockkeyword_binding[]>	Read-only	blockkeyword that can be bound to appfwprofile.
appfwprofile_cmdinjection_binding	<appfwprofile_cmdinjection_binding[]>	Read-only	cmdinjection that can be bound to appfwprofile.
appfwprofile_fakeaccount_binding	<appfwprofile_fakeaccount_binding[]>	Read-only	fakeaccount that can be bound to appfwprofile.
appfwprofile_trustedlearningclients_binding	<appfwprofile_trustedlearningclients_binding[]>	Read-only	trustedlearningclients that can be bound to appfwprofile.
appfwprofile_xmldosurl_binding	<appfwprofile_xmldosurl_binding[]>	Read-only	xmldosurl that can be bound to appfwprofile.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
appfwprofile_fieldconsistency_binding	<appfwprofile_fieldconsistency_binding[]>	Read-only	fieldconsistency that can be bound to appfwprofile.
appfwprofile_restvalidation_binding	<appfwprofile_restvalidation_binding[]>	Read-only	restvalidation that can be bound to appfwprofile.
appfwprofile_fieldformat_binding	<appfwprofile_fieldformat_binding[]>	Read-only	fieldformat that can be bound to appfwprofile.
appfwprofile_xmlattachmenturl_binding	<appfwprofile_xmlattachmenturl_binding[]>	Read-only	xmlattachmenturl that can be bound to appfwprofile.
appfwprofile_denylist_binding	<appfwprofile_denylist_binding[]>	Read-only	denylist that can be bound to appfwprofile.
appfwprofile_appfwconfidfield_binding	<appfwprofile_appfwconfidfield_binding[]>	Read-only	appfwconfidfield that can be bound to appfwprofile.
appfwprofile_csrftag_binding	<appfwprofile_csrftag_binding[]>	Read-only	csrftag that can be bound to appfwprofile.
appfwprofile_crosssitescripting_binding	<appfwprofile_crosssitescripting_binding[]>	Read-only	crosssitescripting that can be bound to appfwprofile.
appfwprofile_safeobject_binding	<appfwprofile_safeobject_binding[]>	Read-only	safeobject that can be bound to appfwprofile.
appfwprofile_xmlwsiurl_binding	<appfwprofile_xmlwsiurl_binding[]>	Read-only	xmlwsiurl that can be bound to appfwprofile.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
appfwprofile_xmlvalidationurl_binding	<appfwprofile_xmlvalidationurl_binding[]>	Read-only	xmlvalidationurl that can be bound to appfwprofile.
appfwprofile_fileuploadtype_binding	<appfwprofile_fileuploadtype_binding[]>	Read-only	fileuploadtype that can be bound to appfwprofile.
appfwprofile_creditcardnumber_binding	<appfwprofile_creditcardnumber_binding[]>	Read-only	creditcardnumber that can be bound to appfwprofile.
appfwprofile_denyurl_binding	<appfwprofile_denyurl_binding[]>	Read-only	denyurl that can be bound to appfwprofile.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_binding/ name_value<String>
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "appfwprofile_binding": [ {

"name":<String_value>,

"appfwprofile_cmdinjection_binding":<appfwprofile_cmdinjection_binding[]_value>,

"appfwprofile_safeobject_binding":<appfwprofile_safeobject_binding[]_value>,

"appfwprofile_denylist_binding":<appfwprofile_denylist_binding[]_value>,

"appfwprofile_fieldconsistency_binding":<appfwprofile_fieldconsistency_binding[]_value>,
```

```
"appfwprofile_xmlattachmenturl_binding":<appfwprofile_xmlattachmenturl_bin
ding[]_value>,

"appfwprofile_bypasslist_binding":<appfwprofile_bypasslist_binding[]_value
>,

"appfwprofile_fileuploadtype_binding":<appfwprofile_fileuploadtype_binding
[]_value>,

"appfwprofile_cookieconsistency_binding":<appfwprofile_cookieconsistency_b
inding[]_value>,

"appfwprofile_appfwconfidfield_binding":<appfwprofile_appfwconfidfield_bin
ding[]_value>,

"appfwprofile_xmlsqlinjection_binding":<appfwprofile_xmlsqlinjection_bindi
ng[]_value>,

"appfwprofile_crosssitescripting_binding":<appfwprofile_crosssitescripting
_binding[]_value>,

"appfwprofile_contenttype_binding":<appfwprofile_contenttype_binding[]_val
ue>,

"appfwprofile_xmlvalidationurl_binding":<appfwprofile_xmlvalidationurl_bin
ding[]_value>,

"appfwprofile_jsonblockkeyword_binding":<appfwprofile_jsonblockkeyword_bin
ding[]_value>,

"appfwprofile_blockkeyword_binding":<appfwprofile_blockkeyword_binding[]_v
alue>,

"appfwprofile_creditcardnumber_binding":<appfwprofile_creditcardnumber_bin
ding[]_value>,

"appfwprofile_starturl_binding":<appfwprofile_starturl_binding[]_value>,

"appfwprofile_jsonxssurl_binding":<appfwprofile_jsonxssurl_binding[]_value
>,

"appfwprofile_denyurl_binding":<appfwprofile_denyurl_binding[]_value>,
```

```
"appfwprofile_csrftag_binding":<appfwprofile_csrftag_binding[]_value>,

"appfwprofile_restvalidation_binding":<appfwprofile_restvalidation_binding
[]_value>,

"appfwprofile_trustedlearningclients_binding":<appfwprofile_trustedlearnin
gclients_binding[]_value>,

"appfwprofile_fieldformat_binding":<appfwprofile_fieldformat_binding[]_val
ue>,

"appfwprofile_xmlxss_binding":<appfwprofile_xmlxss_binding[]_value>,

"appfwprofile_jsonsqlurl_binding":<appfwprofile_jsonsqlurl_binding[]_value
>,

"appfwprofile_jsondosurl_binding":<appfwprofile_jsondosurl_binding[]_value
>,

"appfwprofile_sqlinjection_binding":<appfwprofile_sqlinjection_binding[]_v
alue>,

"appfwprofile_fakeaccount_binding":<appfwprofile_fakeaccount_binding[]_val
ue>,

"appfwprofile_excluderescontenttype_binding":<appfwprofile_excluderesconte
nttype_binding[]_value>,

"appfwprofile_xmldosurl_binding":<appfwprofile_xmldosurl_binding[]_value>,

"appfwprofile_logexpression_binding":<appfwprofile_logexpression_binding[]
_value>,

"appfwprofile_jsoncmdurl_binding":<appfwprofile_jsoncmdurl_binding[]_value
>,

"appfwprofile_xmlwsiurl_binding":<appfwprofile_xmlwsiurl_binding[]_value>,

"appfwprofile_grpcvalidation_binding":<appfwprofile_grpcvalidation_binding
[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "appfwprofile_binding": [ {

"name":<String_value>,

"appfwprofile_cmdinjection_binding":<appfwprofile_cmdinjection_binding[]_value>,

"appfwprofile_safeobject_binding":<appfwprofile_safeobject_binding[]_value>,

"appfwprofile_denylist_binding":<appfwprofile_denylist_binding[]_value>,

"appfwprofile_fieldconsistency_binding":<appfwprofile_fieldconsistency_binding[]_value>,
```

```
"appfwprofile_xmlattachmenturl_binding":<appfwprofile_xmlattachmenturl_bin
ding[]_value>,

"appfwprofile_bypasslist_binding":<appfwprofile_bypasslist_binding[]_value
>,

"appfwprofile_fileuploadtype_binding":<appfwprofile_fileuploadtype_binding
[]_value>,

"appfwprofile_cookieconsistency_binding":<appfwprofile_cookieconsistency_b
inding[]_value>,

"appfwprofile_appfwconfidfield_binding":<appfwprofile_appfwconfidfield_bin
ding[]_value>,

"appfwprofile_xmlsqlinjection_binding":<appfwprofile_xmlsqlinjection_bindi
ng[]_value>,

"appfwprofile_crosssitescripting_binding":<appfwprofile_crosssitescripting
_binding[]_value>,

"appfwprofile_contenttype_binding":<appfwprofile_contenttype_binding[]_val
ue>,

"appfwprofile_xmlvalidationurl_binding":<appfwprofile_xmlvalidationurl_bin
ding[]_value>,

"appfwprofile_jsonblockkeyword_binding":<appfwprofile_jsonblockkeyword_bin
ding[]_value>,

"appfwprofile_blockkeyword_binding":<appfwprofile_blockkeyword_binding[]_v
alue>,

"appfwprofile_creditcardnumber_binding":<appfwprofile_creditcardnumber_bin
ding[]_value>,

"appfwprofile_starturl_binding":<appfwprofile_starturl_binding[]_value>,

"appfwprofile_jsonxssurl_binding":<appfwprofile_jsonxssurl_binding[]_value
>,

"appfwprofile_denyurl_binding":<appfwprofile_denyurl_binding[]_value>,
```

```
"appfwprofile_csrftag_binding":<appfwprofile_csrftag_binding[]_value>,

"appfwprofile_restvalidation_binding":<appfwprofile_restvalidation_binding
[]_value>,

"appfwprofile_trustedlearningclients_binding":<appfwprofile_trustedlearnin
gclients_binding[]_value>,

"appfwprofile_fieldformat_binding":<appfwprofile_fieldformat_binding[]_val
ue>,

"appfwprofile_xmlxss_binding":<appfwprofile_xmlxss_binding[]_value>,

"appfwprofile_jsonsqlurl_binding":<appfwprofile_jsonsqlurl_binding[]_value
>,

"appfwprofile_jsondosurl_binding":<appfwprofile_jsondosurl_binding[]_value
>,

"appfwprofile_sqlinjection_binding":<appfwprofile_sqlinjection_binding[]_v
alue>,

"appfwprofile_fakeaccount_binding":<appfwprofile_fakeaccount_binding[]_val
ue>,

"appfwprofile_excluderescontenttype_binding":<appfwprofile_excluderesconte
nttype_binding[]_value>,

"appfwprofile_xmldosurl_binding":<appfwprofile_xmldosurl_binding[]_value>,

"appfwprofile_logexpression_binding":<appfwprofile_logexpression_binding[]
_value>,

"appfwprofile_jsoncmdurl_binding":<appfwprofile_jsoncmdurl_binding[]_value
>,

"appfwprofile_xmlwsiurl_binding":<appfwprofile_xmlwsiurl_binding[]_value>,

"appfwprofile_grpcvalidation_binding":<appfwprofile_grpcvalidation_binding
[]_value>

}]}
```

appfwprofile_blockkeyword_binding

Binding object showing the blockkeyword that can be bound to appfwprofile.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
fieldname	<String>	Read-write	A block keyword field name.
resourceid	<String>	Read-write	A "id" that identifies the rule.
blockkeyword	<String>	Read-write	Field name of the block keyword binding.
blockkeywordtype	<String>	Read-write	block keyword type(literal|PCRE). Possible values = literal, PCRE
state	<String>	Read-write	Enabled. Possible values = ENABLED, DISABLED
comment	<String>	Read-write	Any comments about the purpose of profile, or other useful information about the profile.
alertonly	<String>	Read-write	Send SNMP alert?. Possible values = ON, OFF

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
as_blockkeyword_formurl	<String>	Read-write	The blockkeyword form action URL.
as_fieldname_isregex_blockkeyword	<String>	Read-write	Is block keyword field name regular expression?. Default value: NOTREGEX Possible values = REGEX, NOTREGEX
name	<String>	Read-write	Name of the profile to which to bind an exemption or rule. Minimum length = 1
isautodeployed	<String>	Read-write	Is the rule auto deployed by dynamic profile ?. Possible values = AUTODEPLOYED, NOTAUTODEPLOYED
ruletype	<String>	Read-write	Specifies rule type of binding. Possible values = ALLOW, DENY
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/appfwprofile_blockkeyword_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"appfwprofile_blockkeyword_binding":{

<b>"name":<String_value>,

</b>"comment":<String_value>,

"state":<String_value>,

"isautodeployed":<String_value>,

"resourceid":<String_value>,

"blockkeyword":<String_value>,

"fieldname":<String_value>,

"as_blockkeyword_formurl":<String_value>,

"as_fieldname_isregex_blockkeyword":<String_value>,

"blockkeywordtype":<String_value>,

"ruletype":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_blockkeyword_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ appfwprofile_blockkeyword_binding/ name_value<String> ? **args=blockkeyword: <String_value> ,fieldname: <String_value> ,as_blockkeyword_formurl: <String_value> ,ruletype: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_blockkeyword_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ appfwprofile_blockkeyword_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of appfwprofile_blockkeyword_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_blockkeyword_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the appfwprofile_blockkeyword_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwprofile_blockkeyword_binding": [ {

"fieldname":<String_value>,

"resourceid":<String_value>,

"blockkeyword":<String_value>,

"blockkeywordtype":<String_value>,

"state":<String_value>,

"comment":<String_value>,

"alertonly":<String_value>,

"as_blockkeyword_formurl":<String_value>,

"as_fieldname_isregex_blockkeyword":<String_value>,

"name":<String_value>,

"isautodeployed":<String_value>,

"ruletype":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_blockkeyword_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_blockkeyword_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwprofile_blockkeyword_binding": [ {

"fieldname":<String_value>,

"resourceid":<String_value>,

"blockkeyword":<String_value>,

"blockkeywordtype":<String_value>,

"state":<String_value>,

"comment":<String_value>,

"alertonly":<String_value>,

"as_blockkeyword_formurl":<String_value>,

"as_fieldname_isregex_blockkeyword":<String_value>,

"name":<String_value>,

"isautodeployed":<String_value>,

"ruletype":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_blockkeyword_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"appfwprofile_blockkeyword_binding": [ { "__count": "#no"} ] }
```

appfwprofile_bypasslist_binding

Binding object showing the bypasslist that can be bound to appfwprofile.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
as_bypass_list_action	<String>	Read-write	Bypass List Action. Possible values = none, log
name	<String>	Read-write	Name of the profile to which to bind an exemption or rule. Minimum length = 1
state	<String>	Read-write	Enabled.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ENABLED, DISABLED
as_bypass_list_value_type	<String>	Read-write	Bypass List value type. Default value: literal Possible values = literal, PCRE, Expression
resourceid	<String>	Read-write	A "id" that identifies the rule.
isautodeployed	<String>	Read-write	Is the rule auto deployed by dynamic profile ?. Possible values = AUTODEPLOYED, NOTAUTODEPLOYED
alertonly	<String>	Read-write	Send SNMP alert?. Possible values = ON, OFF
as_bypass_list	<String>	Read-write	Bypass List Value.
as_bypass_list_location	<String>	Read-write	Bypass List scan location. Possible values = IPv4, IPv6, URL, HeaderName, HeaderValue
ruletype	<String>	Read-write	Specifies rule type of binding.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ALLOW, DENY
comment	<String>	Read-write	Any comments about the purpose of profile, or other useful information about the profile.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/appfwprofile_bypasslist_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"appfwprofile_bypasslist_binding":{

<b>"name":<String_value>,

</b>"comment":<String_value>,

"state":<String_value>,

"isautodeployed":<String_value>,

"resourceid":<String_value>,

"as_bypass_list":<String_value>,

"as_bypass_list_value_type":<String_value>,

"as_bypass_list_action":<String_value>,

"as_bypass_list_location":<String_value>,
```

```
"ruletype":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_bypasslist_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ appfwprofile_bypasslist_binding/ name_value<String> ? **args=as_bypass_list: <String_value> ,as_bypass_list_value_type: <String_value> ,as_bypass_list_location: <String_value> ,ruletype: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_bypasslist_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ appfwprofile_bypasslist_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of appfwprofile_bypasslist_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_bypasslist_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the appfwprofile_bypasslist_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwprofile_bypasslist_binding": [ {

"as_bypass_list_action":<String_value>,

"name":<String_value>,

"state":<String_value>,

"as_bypass_list_value_type":<String_value>,

"resourceid":<String_value>,

"isautodeployed":<String_value>,

"alertonly":<String_value>,

"as_bypass_list":<String_value>,

"as_bypass_list_location":<String_value>,

"ruletype":<String_value>,

"comment":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_bypasslist_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_bypasslist_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwprofile_bypasslist_binding": [ {

"as_bypass_list_action":<String_value>,

"name":<String_value>,

"state":<String_value>,

"as_bypass_list_value_type":<String_value>,

"resourceid":<String_value>,

"isautodeployed":<String_value>,
```

```
"alertonly":<String_value>,

"as_bypass_list":<String_value>,

"as_bypass_list_location":<String_value>,

"ruletype":<String_value>,

"comment":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_bypasslist_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"appfwprofile_bypasslist_binding": [ { "__count": "#no"} ] }
```

appfwprofile_cmdinjection_binding

Binding object showing the cmdinjection that can be bound to appfwprofile.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the profile to which to bind an exemption or rule. Minimum length = 1
state	<String>	Read-write	Enabled. Possible values = ENABLED, DISABLED
as_value_type_cmd	<String>	Read-write	Type of the relaxed web form value. Possible values = Keyword, SpecialString
resourceid	<String>	Read-write	A "id" that identifies the rule.
as_value_expr_cmd	<String>	Read-write	The web form/ header/cookie value expression.
ruletype	<String>	Read-write	Specifies rule type of binding. Possible values = ALLOW, DENY
isvalueregex_cmd	<String>	Read-write	Is the web form field/ header/cookie value a regular expression?. Possible values = REGEX, NOTREGEX

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
isregex_cmd	<String>	Read-write	Is the relaxed web form field name/ header/cookie a regular expression?. Possible values = REGEX, NOTREGEX
cmdinjection	<String>	Read-write	Name of the relaxed web form field/ header/cookie.
comment	<String>	Read-write	Any comments about the purpose of profile, or other useful information about the profile.
formactionurl_cmd	<String>	Read-write	The web form action URL.
isautodeployed	<String>	Read-write	Is the rule auto deployed by dynamic profile ?. Possible values = AUTODEPLOYED, NOTAUTODEPLOYED
as_scan_location_cmd	<String>	Read-write	Location of command injection exception - form field, header or cookie. Possible values = FORMFIELD, HEADER, COOKIE
alertonly	<String>	Read-write	Send SNMP alert?.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ON, OFF
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/appfwprofile_cmdinjection_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"appfwprofile_cmdinjection_binding":{

<b>"name":<String_value>,

</b>"cmdinjection":<String_value>,

"formactionurl_cmd":<String_value>,

"isregex_cmd":<String_value>,

"as_scan_location_cmd":<String_value>,

"as_value_type_cmd":<String_value>,

"as_value_expr_cmd":<String_value>,

"isvalueregex_cmd":<String_value>,

"comment":<String_value>,

"state":<String_value>,

"isautodeployed":<String_value>,

"resourceid":<String_value>,

"ruletype":<String_value>
```

```
}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_cmdinjection_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ appfwprofile_cmdinjection_binding/ name_value<String> ? **args=cmdinjection: <String_value> ,formactionurl_cmd: <String_value> ,as_scan_location_cmd: <String_value> ,as_value_type_cmd: <String_value> ,as_value_expr_cmd: <String_value> ,ruletype: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_cmdinjection_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ appfwprofile_cmdinjection_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of appfwprofile_cmdinjection_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_cmdinjection_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the appfwprofile_cmdinjection_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwprofile_cmdinjection_binding": [ {

"name":<String_value>,

"state":<String_value>,

"as_value_type_cmd":<String_value>,

"resourceid":<String_value>,

"as_value_expr_cmd":<String_value>,

"ruletype":<String_value>,

"isvalueregex_cmd":<String_value>,

"isregex_cmd":<String_value>,

"cmdinjection":<String_value>,

"comment":<String_value>,

"formactionurl_cmd":<String_value>,

"isautodeployed":<String_value>,

"as_scan_location_cmd":<String_value>,
```

```
"alertonly":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_cmdinjection_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_cmdinjection_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwprofile_cmdinjection_binding": [ {

"name":<String_value>,

"state":<String_value>,

"as_value_type_cmd":<String_value>,

"resourceid":<String_value>,
```

```
"as_value_expr_cmd":<String_value>,

"ruletype":<String_value>,

"isvalueregex_cmd":<String_value>,

"isregex_cmd":<String_value>,

"cmdinjection":<String_value>,

"comment":<String_value>,

"formactionurl_cmd":<String_value>,

"isautodeployed":<String_value>,

"as_scan_location_cmd":<String_value>,

"alertonly":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_cmdinjection_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"appfwprofile_cmdinjection_binding": [ { "__count": "#no"} ] }
```

appfwprofile_contenttype_binding

Binding object showing the contenttype that can be bound to appfwprofile.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ruletype	<String>	Read-write	Specifies rule type of binding. Possible values = ALLOW, DENY
comment	<String>	Read-write	Any comments about the purpose of profile, or other useful information about the profile.
alertonly	<String>	Read-write	Send SNMP alert?. Possible values = ON, OFF
isautodeployed	<String>	Read-write	Is the rule auto deployed by dynamic profile ?. Possible values = AUTODEPLOYED, NOTAUTODEPLOYED
contenttype	<String>	Read-write	A regular expression that designates a content-type on the content-types list.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the profile to which to bind an exemption or rule. Minimum length = 1
resourceid	<String>	Read-write	A "id" that identifies the rule.
state	<String>	Read-write	Enabled. Possible values = ENABLED, DISABLED
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of

creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/appfwprofile_contenttype_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"appfwprofile_contenttype_binding":{

<b>"name":<String_value>,

</b>"comment":<String_value>,

"state":<String_value>,

"contenttype":<String_value>,

"isautodeployed":<String_value>,

"resourceid":<String_value>,
```

```
"ruletype":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_contenttype_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ appfwprofile_contenttype_binding/ name_value<String> ? **args=contenttype: <String_value> ,ruletype: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_contenttype_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ appfwprofile_contenttype_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of appfwprofile_contenttype_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_contenttype_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the appfwprofile_contenttype_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwprofile_contenttype_binding": [ {

"ruletype":<String_value>,

"comment":<String_value>,

"alertonly":<String_value>,

"isautodeployed":<String_value>,

"contenttype":<String_value>,

"name":<String_value>,

"resourceid":<String_value>,

"state":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_contenttype_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_contenttype_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwprofile_contenttype_binding": [ {

"ruletype":<String_value>,

"comment":<String_value>,

"alertonly":<String_value>,

"isautodeployed":<String_value>,

"contenttype":<String_value>,

"name":<String_value>,

"resourceid":<String_value>,

"state":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_contenttype_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"appfwprofile_contenttype_binding": [ { "__count": "#no"} ] }
```

appfwprofile_cookieconsistency_binding

Binding object showing the cookieconsistency that can be bound to appfwprofile.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
isregex	<String>	Read-write	Is the cookie name a regular expression?. Possible values = REGEX, NOTREGEX
state	<String>	Read-write	Enabled.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ENABLED, DISABLED
resourceid	<String>	Read-write	A "id" that identifies the rule.
name	<String>	Read-write	Name of the profile to which to bind an exemption or rule. Minimum length = 1
isautodeployed	<String>	Read-write	Is the rule auto deployed by dynamic profile ?. Possible values = AUTODEPLOYED, NOTAUTODEPLOYED
alertonly	<String>	Read-write	Send SNMP alert?. Possible values = ON, OFF
comment	<String>	Read-write	Any comments about the purpose of profile, or other useful information about the profile.
ruletype	<String>	Read-write	Specifies rule type of binding. Possible values = ALLOW, DENY
cookieconsistency	<String>	Read-write	The name of the cookie to be checked.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/appfwprofile_cookieconsistency_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"appfwprofile_cookieconsistency_binding":{

<b>"name":<String_value>,

</b>"cookieconsistency":<String_value>,

"isregex":<String_value>,

"comment":<String_value>,

"state":<String_value>,

"isautodeployed":<String_value>,

"resourceid":<String_value>,

"ruletype":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_cookieconsistency_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ appfwprofile_cookieconsistency_binding/ name_value<String> ? **args=cookieconsistency: <String_value> ,ruletype: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_cookieconsistency_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ appfwprofile_cookieconsistency_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of appfwprofile_cookieconsistency_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_cookieconsistency_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the appfwprofile_cookieconsistency_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwprofile_cookieconsistency_binding": [ {

"isregex":<String_value>,
```

```
"state":<String_value>,

"resourceid":<String_value>,

"name":<String_value>,

"isautodeployed":<String_value>,

"alertonly":<String_value>,

"comment":<String_value>,

"ruletype":<String_value>,

"cookieconsistency":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_cookieconsistency_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_cookieconsistency_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwprofile_cookieconsistency_binding": [ {

"isregex":<String_value>,

"state":<String_value>,

"resourceid":<String_value>,

"name":<String_value>,

"isautodeployed":<String_value>,

"alertonly":<String_value>,

"comment":<String_value>,

"ruletype":<String_value>,

"cookieconsistency":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_cookieconsistency_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"appfwprofile_cookieconsistency_binding": [ { "__count": "#no"} ] }
```

appfwprofile_creditcardnumber_binding

Binding object showing the creditcardnumber that can be bound to appfwprofile.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
state	<String>	Read-write	Enabled. Possible values = ENABLED, DISABLED
comment	<String>	Read-write	Any comments about the purpose of profile, or other useful information about the profile.
resourceid	<String>	Read-write	A "id" that identifies the rule.
creditcardnumber	<String>	Read-write	The object expression that is to be excluded from safe commerce check.
ruletype	<String>	Read-write	Specifies rule type of binding. Possible values = ALLOW, DENY

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the profile to which to bind an exemption or rule. Minimum length = 1
isautodeployed	<String>	Read-write	Is the rule auto deployed by dynamic profile ?. Possible values = AUTODEPLOYED, NOTAUTODEPLOYED
alertonly	<String>	Read-write	Send SNMP alert?. Possible values = ON, OFF
creditcardnumberurl	<String>	Read-write	The url for which the list of credit card numbers are needed to be bypassed from inspection.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/appfwprofile_creditcardnumber_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"appfwprofile_creditcardnumber_binding":{

<b>"name":<String_value>,
```

```
</b>"comment":<String_value>,

"state":<String_value>,

"creditcardnumber":<String_value>,

"creditcardnumberurl":<String_value>,

"isautodeployed":<String_value>,

"resourceid":<String_value>,

"ruletype":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_creditcardnumber_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ appfwprofile_creditcardnumber_binding/ name_value<String> ? **args=creditcardnumber: <String_value> ,creditcardnumberurl: <String_value> ,ruletype: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_creditcardnumber_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/

appfwprofile_creditcardnumber_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of appfwprofile_creditcardnumber_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_creditcardnumber_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the appfwprofile_creditcardnumber_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwprofile_creditcardnumber_binding": [ {

"state":<String_value>,

"comment":<String_value>,

"resourceid":<String_value>,

"creditcardnumber":<String_value>,

"ruletype":<String_value>,

"name":<String_value>,
```

```
"isautodeployed":<String_value>,

"alertonly":<String_value>,

"creditcardnumberurl":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_creditcardnumber_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_creditcardnumber_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwprofile_creditcardnumber_binding": [ {

"state":<String_value>,

"comment":<String_value>,
```

```
"resourceid":<String_value>,

"creditcardnumber":<String_value>,

"ruletype":<String_value>,

"name":<String_value>,

"isautodeployed":<String_value>,

"alertonly":<String_value>,

"creditcardnumberurl":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_creditcardnumber_binding/name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"appfwprofile_creditcardnumber_binding": [ { "__count": "#no"} ] }
```

appfwprofile_crosssitescripting_binding

Binding object showing the crosssitescripting that can be bound to appfwprofile.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
alertonly	<String>	Read-write	Send SNMP alert?. Possible values = ON, OFF
as_value_expr_xss	<String>	Read-write	The web form value expression.
as_scan_location_xss	<String>	Read-write	Location of cross-site scripting exception - form field, header, cookie or URL. Possible values = FORMFIELD, HEADER, COOKIE, URL
ruletype	<String>	Read-write	Specifies rule type of binding. Possible values = ALLOW, DENY
name	<String>	Read-write	Name of the profile to which to bind an exemption or rule. Minimum length = 1
isautodeployed	<String>	Read-write	Is the rule auto deployed by dynamic profile ?. Possible values = AUTODEPLOYED,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			NOTAUTODEPLOYED
isregex_xss	<String>	Read-write	Is the web form field name a regular expression?. Possible values = REGEX, NOTREGEX
crosssitescripting	<String>	Read-write	The web form field name.
resourceid	<String>	Read-write	A "id" that identifies the rule.
state	<String>	Read-write	Enabled. Possible values = ENABLED, DISABLED
comment	<String>	Read-write	Any comments about the purpose of profile, or other useful information about the profile.
as_value_type_xss	<String>	Read-write	The web form value type. Possible values = Tag, Attribute, Pattern
formactionurl_xss	<String>	Read-write	The web form action URL.
isvalueregex_xss	<String>	Read-write	Is the web form field value a regular expression?.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = REGEX, NOTREGEX
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/appfwprofile_crosssitescripting_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"appfwprofile_crosssitescripting_binding":{

<b>"name":<String_value>,

</b>"crosssitescripting":<String_value>,

"formactionurl_xss":<String_value>,

"isregex_xss":<String_value>,

"as_scan_location_xss":<String_value>,

"as_value_type_xss":<String_value>,

"as_value_expr_xss":<String_value>,

"isvalueregex_xss":<String_value>,

"comment":<String_value>,

"state":<String_value>,

"isautodeployed":<String_value>,

"resourceid":<String_value>,
```

```
"ruletype":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_crosssitescripting_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ appfwprofile_crosssitescripting_binding/ name_value<String> ? **args=crosssitescripting: <String_value> ,formactionurl_xss: <String_value> ,as_scan_location_xss: <String_value> ,as_value_type_xss: <String_value> ,as_value_expr_xss: <String_value> ,ruletype: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_crosssitescripting_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ appfwprofile_crosssitescripting_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of appfwprofile_crosssitescripting_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_crosssitescripting_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the appfwprofile_crosssitescripting_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwprofile_crosssitescripting_binding": [ {

"alertonly":<String_value>,

"as_value_expr_xss":<String_value>,

"as_scan_location_xss":<String_value>,

"ruletype":<String_value>,

"name":<String_value>,

"isautodeployed":<String_value>,

"isregex_xss":<String_value>,

"crosssitescripting":<String_value>,

"resourceid":<String_value>,

"state":<String_value>,

"comment":<String_value>,

"as_value_type_xss":<String_value>,
```

```
"formactionurl_xss":<String_value>,

"isvalueregex_xss":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_crosssitescripting_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_crosssitescripting_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwprofile_crosssitescripting_binding": [ {

"alertonly":<String_value>,

"as_value_expr_xss":<String_value>,

"as_scan_location_xss":<String_value>,
```

```
"ruletype":<String_value>,

"name":<String_value>,

"isautodeployed":<String_value>,

"isregex_xss":<String_value>,

"crosssitescripting":<String_value>,

"resourceid":<String_value>,

"state":<String_value>,

"comment":<String_value>,

"as_value_type_xss":<String_value>,

"formactionurl_xss":<String_value>,

"isvalueregex_xss":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_crosssitescripting_binding/name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"appfwprofile_crosssitescripting_binding": [ { "__count": "#no"} ] }
```

appfwprofile_csrftag_binding

Binding object showing the csrftag that can be bound to appfwprofile.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
comment	<String>	Read-write	Any comments about the purpose of profile, or other useful information about the profile.
state	<String>	Read-write	Enabled. Possible values = ENABLED, DISABLED
csrfformactionurl	<String>	Read-write	The web form action URL.
resourceid	<String>	Read-write	A "id" that identifies the rule.
ruletype	<String>	Read-write	Specifies rule type of binding. Possible values = ALLOW, DENY
csrftag	<String>	Read-write	The web form originating URL.
name	<String>	Read-write	Name of the profile to which to bind an exemption or rule.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum length = 1
isautodeployed	<String>	Read-write	Is the rule auto deployed by dynamic profile ?. Possible values = AUTODEPLOYED, NOTAUTODEPLOYED
alertonly	<String>	Read-write	Send SNMP alert?. Possible values = ON, OFF
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of

creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/appfwprofile_csrftag_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"appfwprofile_csrftag_binding":{

<b>"name":<String_value>,

</b>"csrftag":<String_value>,

"csrfformactionurl":<String_value>,

"comment":<String_value>,

"state":<String_value>,

"isautodeployed":<String_value>,
```

```
"resourceid":<String_value>,

"ruletype":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_csrftag_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ appfwprofile_csrftag_binding/ name_value<String> ? **args=csrftag: <String_value> ,csrfformactionurl: <String_value> ,ruletype: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_csrftag_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ appfwprofile_csrftag_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of appfwprofile_csrftag_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_csrftag_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the appfwprofile_csrftag_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwprofile_csrftag_binding": [ {

"comment":<String_value>,

"state":<String_value>,

"csrfformactionurl":<String_value>,

"resourceid":<String_value>,

"ruletype":<String_value>,

"csrftag":<String_value>,

"name":<String_value>,

"isautodeployed":<String_value>,

"alertonly":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_csrftag_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_csrftag_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwprofile_csrftag_binding": [ {

"comment":<String_value>,

"state":<String_value>,

"csrfformactionurl":<String_value>,

"resourceid":<String_value>,

"ruletype":<String_value>,

"csrftag":<String_value>,

"name":<String_value>,
```

```
"isautodeployed":<String_value>,

"alertonly":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_csrftag_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"appfwprofile_csrftag_binding": [ { "__count": "#no"} ] }
```

appfwprofile_denylist_binding

Binding object showing the denylist that can be bound to appfwprofile.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
resourceid	<String>	Read-write	A "id" that identifies the rule.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
as_deny_list_value_type	<String>	Read-write	Deny List value type. Default value: literal Possible values = literal, PCRE, Expression
as_deny_list_action	<String[]>	Read-write	Deny List Action. Default value = REDIRECT. Default value: REDIRECT Possible values = none, log, RESET, REDIRECT
comment	<String>	Read-write	Any comments about the purpose of profile, or other useful information about the profile.
state	<String>	Read-write	Enabled. Possible values = ENABLED, DISABLED
as_deny_list_location	<String>	Read-write	Deny List scan location. Possible values = IPv4, IPv6, URL, HeaderName, HeaderValue
alertonly	<String>	Read-write	Send SNMP alert?. Possible values = ON, OFF

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
isautodeployed	<String>	Read-write	Is the rule auto deployed by dynamic profile ?. Possible values = AUTODEPLOYED, NOTAUTODEPLOYED
name	<String>	Read-write	Name of the profile to which to bind an exemption or rule. Minimum length = 1
ruletype	<String>	Read-write	Specifies rule type of binding. Possible values = ALLOW, DENY
as_deny_list	<String>	Read-write	Deny List Value.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/appfwprofile_denylist_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"appfwprofile_denylist_binding":{

<b>"name":<String_value>,

</b>"comment":<String_value>,

"state":<String_value>,

"isautodeployed":<String_value>,
```

```
"resourceid":<String_value>,

"as_deny_list":<String_value>,

"as_deny_list_value_type":<String_value>,

"as_deny_list_action":<String[]_value>,

"as_deny_list_location":<String_value>,

"ruletype":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_denylist_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ appfwprofile_denylist_binding/ name_value<String> ? **args=as_deny_list: <String_value> ,as_deny_list_value_type: <String_value> ,as_deny_list_location: <String_value> ,ruletype: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_denylist_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/

appfwprofile_denylist_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of appfwprofile_denylist_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_denylist_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the appfwprofile_denylist_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwprofile_denylist_binding": [ {

"resourceid":<String_value>,

"as_deny_list_value_type":<String_value>,

"as_deny_list_action":<String[]_value>,

"comment":<String_value>,

"state":<String_value>,

"as_deny_list_location":<String_value>,
```

```
"alertonly":<String_value>,

"isautodeployed":<String_value>,

"name":<String_value>,

"ruletype":<String_value>,

"as_deny_list":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_denylist_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_denylist_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwprofile_denylist_binding": [ {

"resourceid":<String_value>,

"as_deny_list_value_type":<String_value>,

"as_deny_list_action":<String[]_value>,

"comment":<String_value>,

"state":<String_value>,

"as_deny_list_location":<String_value>,

"alertonly":<String_value>,

"isautodeployed":<String_value>,

"name":<String_value>,

"ruletype":<String_value>,

"as_deny_list":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_denylist_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"appfwprofile_denylist_binding": [ { "__count": "#no"} ] }
```

appfwprofile_denyurl_binding

Binding object showing the denyurl that can be bound to appfwprofile.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
alertonly	<String>	Read-write	Send SNMP alert?. Possible values = ON, OFF
ruletype	<String>	Read-write	Specifies rule type of binding. Possible values = ALLOW, DENY
isautodeployed	<String>	Read-write	Is the rule auto deployed by dynamic profile ?. Possible values = AUTODEPLOYED, NOTAUTODEPLOYED
name	<String>	Read-write	Name of the profile to which to bind an exemption or rule. Minimum length = 1
resourceid	<String>	Read-write	A "id" that identifies the rule.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
comment	<String>	Read-write	Any comments about the purpose of profile, or other useful information about the profile.
denyurl	<String>	Read-write	A regular expression that designates a URL on the Deny URL list.
state	<String>	Read-write	Enabled. Possible values = ENABLED, DISABLED
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/appfwprofile_denyurl_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"appfwprofile_denyurl_binding":{

<b>"name":<String_value>,

</b>"denyurl":<String_value>,

"comment":<String_value>,

"state":<String_value>,

"isautodeployed":<String_value>,
```

```
"resourceid":<String_value>,

"ruletype":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_denyurl_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ appfwprofile_denyurl_binding/ name_value<String> ? **args=denyurl: <String_value> ,ruletype: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_denyurl_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ appfwprofile_denyurl_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of appfwprofile_denyurl_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_denyurl_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the appfwprofile_denyurl_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwprofile_denyurl_binding": [ {

"alertonly":<String_value>,

"ruletype":<String_value>,

"isautodeployed":<String_value>,

"name":<String_value>,

"resourceid":<String_value>,

"comment":<String_value>,

"denyurl":<String_value>,

"state":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_denyurl_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ appfwprofile_denyurl_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwprofile_denyurl_binding": [ {

"alertonly":<String_value>,

"ruletype":<String_value>,

"isautodeployed":<String_value>,

"name":<String_value>,

"resourceid":<String_value>,

"comment":<String_value>,

"denyurl":<String_value>,

"state":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_denyurl_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"appfwprofile_denyurl_binding": [ { "__count": "#no"} ] }
```

appfwprofile_excluderescontenttype_binding

Binding object showing the excluderescontenttype that can be bound to appfwprofile.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
excluderescontenttype	<String>	Read-write	A regular expression that represents the content type of the response that are to be excluded from inspection.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ruletype	<String>	Read-write	Specifies rule type of binding. Possible values = ALLOW, DENY
comment	<String>	Read-write	Any comments about the purpose of profile, or other useful information about the profile.
alertonly	<String>	Read-write	Send SNMP alert?. Possible values = ON, OFF
isautodeployed	<String>	Read-write	Is the rule auto deployed by dynamic profile ?. Possible values = AUTODEPLOYED, NOTAUTODEPLOYED
name	<String>	Read-write	Name of the profile to which to bind an exemption or rule. Minimum length = 1
resourceid	<String>	Read-write	A "id" that identifies the rule.
state	<String>	Read-write	Enabled. Possible values = ENABLED, DISABLED
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/appfwprofile_excluderescontenttype_binding
HTTP Method: PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"appfwprofile_excluderescontenttype_binding":{

<b>"name":<String_value>,

</b>"comment":<String_value>,

"state":<String_value>,

"excluderescontenttype":<String_value>,

"isautodeployed":<String_value>,

"resourceid":<String_value>,

"ruletype":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_excluderescontenttype_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ appfwprofile_excluderescontenttype_binding/ name_value<String> ? **args=excluderescontenttype: <String_value> ,ruletype: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_excluderescontenttype_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ appfwprofile_excluderescontenttype_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of appfwprofile_excluderescontenttype_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ appfwprofile_excluderescontenttype_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the appfwprofile_excluderescontenttype_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwprofile_excluderescontenttype_binding": [ {

"excluderescontenttype":<String_value>,

"ruletype":<String_value>,
```

```
"comment":<String_value>,

"alertonly":<String_value>,

"isautodeployed":<String_value>,

"name":<String_value>,

"resourceid":<String_value>,

"state":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_excluderescontenttype_binding
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_excluderescontenttype_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwprofile_excluderescontenttype_binding": [ {

"excluderescontenttype":<String_value>,

"ruletype":<String_value>,

"comment":<String_value>,

"alertonly":<String_value>,

"isautodeployed":<String_value>,

"name":<String_value>,

"resourceid":<String_value>,

"state":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_excluderescontenttype_binding/name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"appfwprofile_excluderescontenttype_binding": [ { "__count": "#no"} ] }
```

appfwprofile_fakeaccount_binding

Binding object showing the fakeaccount that can be bound to appfwprofile.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ruletype	<String>	Read-write	Specifies rule type of binding. Possible values = ALLOW, DENY
name	<String>	Read-write	Name of the profile to which to bind an exemption or rule. Minimum length = 1
isautodeployed	<String>	Read-write	Is the rule auto deployed by dynamic profile ?. Possible values = AUTODEPLOYED, NOTAUTODEPLOYED
formurl_fad	<String>	Read-write	The fake account detection URL.
formexpression	<String>	Read-write	A regular expression that defines the Fake Account.
isfieldnameregex	<String>	Read-write	Is Fake Account Detection field name regex?.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = REGEX, NOTREGEX
alertonly	<String>	Read-write	Send SNMP alert?. Possible values = ON, OFF
fakeaccount	<String>	Read-write	Field name of the fake account rule.
comment	<String>	Read-write	Any comments about the purpose of profile, or other useful information about the profile.
state	<String>	Read-write	Enabled. Possible values = ENABLED, DISABLED
tag	<String>	Read-write	A tag expression that defines the Fake Account.
resourceid	<String>	Read-write	A "id" that identifies the rule.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)

- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/appfwprofile_fakeaccount_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"appfwprofile_fakeaccount_binding":{

<b>"name":<String_value>,

</b>"comment":<String_value>,

"state":<String_value>,

"isautodeployed":<String_value>,

"resourceid":<String_value>,

"fakeaccount":<String_value>,

"tag":<String_value>,

"isfieldnameregex":<String_value>,

"formexpression":<String_value>,

"formurl_fad":<String_value>,

"ruletype":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_fakeaccount_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ appfwprofile_fakeaccount_binding/ name_value<String> ? **args=fakeaccount: <String_value> ,tag: <String_value> ,formexpression: <String_value> ,formurl_fad: <String_value> ,ruletype: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_fakeaccount_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ appfwprofile_fakeaccount_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of appfwprofile_fakeaccount_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_fakeaccount_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the appfwprofile_fakeaccount_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwprofile_fakeaccount_binding": [ {

"ruletype":<String_value>,

"name":<String_value>,

"isautodeployed":<String_value>,

"formurl_fad":<String_value>,

"formexpression":<String_value>,

"isfieldnameregex":<String_value>,

"alertonly":<String_value>,

"fakeaccount":<String_value>,

"comment":<String_value>,

"state":<String_value>,

"tag":<String_value>,

"resourceid":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_fakeaccount_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_fakeaccount_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwprofile_fakeaccount_binding": [ {

"ruletype":<String_value>,

"name":<String_value>,

"isautodeployed":<String_value>,

"formurl_fad":<String_value>,

"formexpression":<String_value>,

"isfieldnameregex":<String_value>,

"alertonly":<String_value>,

"fakeaccount":<String_value>,

"comment":<String_value>,

"state":<String_value>,

"tag":<String_value>,

"resourceid":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_fakeaccount_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"appfwprofile_fakeaccount_binding": [ { "__count": "#no"} ] }
```

appfwprofile_fieldconsistency_binding

Binding object showing the fieldconsistency that can be bound to appfwprofile.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ruletype	<String>	Read-write	Specifies rule type of binding. Possible values = ALLOW, DENY
name	<String>	Read-write	Name of the profile to which to bind an exemption or rule. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
isautodeployed	<String>	Read-write	Is the rule auto deployed by dynamic profile ?. Possible values = AUTODEPLOYED, NOTAUTODEPLOYED
formactionurl_ffc	<String>	Read-write	The web form action URL.
isregex_ffc	<String>	Read-write	Is the web form field name a regular expression?. Possible values = REGEX, NOTREGEX
fieldconsistency	<String>	Read-write	The web form field name.
alertonly	<String>	Read-write	Send SNMP alert?. Possible values = ON, OFF
comment	<String>	Read-write	Any comments about the purpose of profile, or other useful information about the profile.
state	<String>	Read-write	Enabled. Possible values = ENABLED, DISABLED
resourceid	<String>	Read-write	A "id" that identifies the rule.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/appfwprofile_fieldconsistency_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"appfwprofile_fieldconsistency_binding":{

<b>"name":<String_value>,

</b>"fieldconsistency":<String_value>,

"formactionurl_ffc":<String_value>,

"isregex_ffc":<String_value>,

"comment":<String_value>,

"state":<String_value>,

"isautodeployed":<String_value>,

"resourceid":<String_value>,

"ruletype":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_fieldconsistency_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ appfwprofile_fieldconsistency_binding/ name_value<String> ? **args=fieldconsistency: <String_value> ,formactionurl_ffc: <String_value> ,ruletype: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_fieldconsistency_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ appfwprofile_fieldconsistency_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of appfwprofile_fieldconsistency_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_fieldconsistency_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the appfwprofile_fieldconsistency_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwprofile_fieldconsistency_binding": [ {

"ruletype":<String_value>,

"name":<String_value>,

"isautodeployed":<String_value>,

"formactionurl_ffc":<String_value>,

"isregex_ffc":<String_value>,

"fieldconsistency":<String_value>,

"alertonly":<String_value>,

"comment":<String_value>,

"state":<String_value>,

"resourceid":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_fieldconsistency_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_fieldconsistency_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwprofile_fieldconsistency_binding": [ {

"ruletype":<String_value>,

"name":<String_value>,

"isautodeployed":<String_value>,

"formactionurl_ffc":<String_value>,

"isregex_ffc":<String_value>,

"fieldconsistency":<String_value>,

"alertonly":<String_value>,

"comment":<String_value>,

"state":<String_value>,

"resourceid":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_fieldconsistency_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"appfwprofile_fieldconsistency_binding": [ { "__count": "#no"} ] }
```

appfwprofile_fieldformat_binding

Binding object showing the fieldformat that can be bound to appfwprofile.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
alertonly	<String>	Read-write	Send SNMP alert?. Possible values = ON, OFF
fieldformat	<String>	Read-write	Name of the form field to which a field format will be assigned.
formactionurl_ff	<String>	Read-write	Action URL of the form field to which a field format will be assigned.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ruletype	<String>	Read-write	Specifies rule type of binding. Possible values = ALLOW, DENY
isautodeployed	<String>	Read-write	Is the rule auto deployed by dynamic profile ?. Possible values = AUTODEPLOYED, NOTAUTODEPLOYED
name	<String>	Read-write	Name of the profile to which to bind an exemption or rule. Minimum length = 1
resourceid	<String>	Read-write	A "id" that identifies the rule.
fieldtype	<String>	Read-write	The field type you are assigning to this form field.
fieldformatmaxlength	<Integer>	Read-write	The maximum allowed length for data in this form field.
fieldformatminlength	<Integer>	Read-write	The minimum allowed length for data in this form field.
isregex_ff	<String>	Read-write	Is the form field name a regular expression?.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = REGEX, NOTREGEX
state	<String>	Read-write	Enabled. Possible values = ENABLED, DISABLED
comment	<String>	Read-write	Any comments about the purpose of profile, or other useful information about the profile.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/appfwprofile_fieldformat_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"appfwprofile_fieldformat_binding":{

<b>"name":<String_value>,

</b>"fieldformat":<String_value>,

"formactionurl_ff":<String_value>,

"fieldtype":<String_value>,

"fieldformatminlength":<Integer_value>,
```

```
"fieldformatmaxlength":<Integer_value>,

"isregex_ff":<String_value>,

"comment":<String_value>,

"state":<String_value>,

"isautodeployed":<String_value>,

"resourceid":<String_value>,

"ruletype":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_fieldformat_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ appfwprofile_fieldformat_binding/ name_value<String> ? **args=fieldformat: <String_value> ,formactionurl_ff: <String_value> ,ruletype: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_fieldformat_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/

appfwprofile_fieldformat_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of appfwprofile_fieldformat_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_fieldformat_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the appfwprofile_fieldformat_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwprofile_fieldformat_binding": [ {

"alertonly":<String_value>,

"fieldformat":<String_value>,

"formactionurl_ff":<String_value>,

"ruletype":<String_value>,

"isautodeployed":<String_value>,

"name":<String_value>,
```

```
"resourceid":<String_value>,

"fieldtype":<String_value>,

"fieldformatmaxlength":<Integer_value>,

"fieldformatminlength":<Integer_value>,

"isregex_ff":<String_value>,

"state":<String_value>,

"comment":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_fieldformat_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_fieldformat_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwprofile_fieldformat_binding": [ {

"alertonly":<String_value>,

"fieldformat":<String_value>,

"formactionurl_ff":<String_value>,

"ruletype":<String_value>,

"isautodeployed":<String_value>,

"name":<String_value>,

"resourceid":<String_value>,

"fieldtype":<String_value>,

"fieldformatmaxlength":<Integer_value>,

"fieldformatminlength":<Integer_value>,

"isregex_ff":<String_value>,

"state":<String_value>,

"comment":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_fieldformat_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"appfwprofile_fieldformat_binding": [ { "__count": "#no"} ] }
```

appfwprofile_fileuploadtype_binding

Binding object showing the fileuploadtype that can be bound to appfwprofile.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
fileuploadtype	<String>	Read-write	FileUploadTypes to allow/deny.
resourceid	<String>	Read-write	A "id" that identifies the rule.
as_fileuploadtypes_url	<String>	Read-write	FileUploadTypes action URL.
state	<String>	Read-write	Enabled. Possible values = ENABLED, DISABLED
comment	<String>	Read-write	Any comments about the purpose of profile, or other useful information about the profile.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
filetype	<String[]>	Read-write	FileUploadTypes file types. Possible values = pdf, msdoc, text, image, any
isnameregex	<String>	Read-write	Is field name a regular expression?. Default value: NOTREGEX Possible values = REGEX, NOTREGEX
isregex_fileuploadtypes_url	<String>	Read-write	Is a regular expression?. Possible values = REGEX, NOTREGEX
alertonly	<String>	Read-write	Send SNMP alert?. Possible values = ON, OFF
name	<String>	Read-write	Name of the profile to which to bind an exemption or rule. Minimum length = 1
isautodeployed	<String>	Read-write	Is the rule auto deployed by dynamic profile ?. Possible values = AUTODEPLOYED, NOTAUTODEPLOYED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ruletype	<String>	Read-write	Specifies rule type of binding. Possible values = ALLOW, DENY
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/appfwprofile_fileuploadtype_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"appfwprofile_fileuploadtype_binding":{

<b>"name":<String_value>,

</b>"comment":<String_value>,

"state":<String_value>,

"fileuploadtype":<String_value>,

"as_fileuploadtypes_url":<String_value>,

"isnameregex":<String_value>,

"isregex_fileuploadtypes_url":<String_value>,

"filetype":<String[]_value>,

"isautodeployed":<String_value>,

"resourceid":<String_value>,

"ruletype":<String_value>
```

```
}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_fileuploadtype_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ appfwprofile_fileuploadtype_binding/ name_value<String> ? **args=fileuploadtype: <String_value> ,as_fileuploadtypes_url: <String_value> ,filetype: <String_value> ,ruletype: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_fileuploadtype_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ appfwprofile_fileuploadtype_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of appfwprofile_fileuploadtype_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_fileuploadtype_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the appfwprofile_fileuploadtype_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwprofile_fileuploadtype_binding": [ {

"fileuploadtype":<String_value>,

"resourceid":<String_value>,

"as_fileuploadtypes_url":<String_value>,

"state":<String_value>,

"comment":<String_value>,

"filetype":<String[]_value>,

"isnameregex":<String_value>,

"isregex_fileuploadtypes_url":<String_value>,

"alertonly":<String_value>,

"name":<String_value>,

"isautodeployed":<String_value>,

"ruletype":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_fileuploadtype_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_fileuploadtype_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwprofile_fileuploadtype_binding": [ {

"fileuploadtype":<String_value>,

"resourceid":<String_value>,

"as_fileuploadtypes_url":<String_value>,

"state":<String_value>,

"comment":<String_value>,

"filetype":<String[]_value>,
```

```
"isnameregex":<String_value>,

"isregex_fileuploadtypes_url":<String_value>,

"alertonly":<String_value>,

"name":<String_value>,

"isautodeployed":<String_value>,

"ruletype":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_fileuploadtype_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"appfwprofile_fileuploadtype_binding": [ { "__count": "#no"} ] }
```

appfwprofile_grpcvalidation_binding

Binding object showing the grpcvalidation that can be bound to appfwprofile.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
alertonly	<String>	Read-write	Send SNMP alert?. Possible values = ON, OFF
grpc_relax_validation_action	<String>	Read-write	Action to be taken for traffic matching the configured relaxation rule. Default value: none Possible values = log, none
isautodeployed	<String>	Read-write	Is the rule auto deployed by dynamic profile ?. Possible values = AUTODEPLOYED, NOTAUTODEPLOYED
comment	<String>	Read-write	Any comments about the purpose of profile, or other useful information about the profile.
ruletype	<String>	Read-write	Specifies rule type of binding. Possible values = ALLOW, DENY
grpcvalidation	<String>	Read-write	Exempt any gRPC method matching the given pattern from the API schema validation check.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Example: bookstore.api.doc.AddBook.
resourceid	<String>	Read-write	A "id" that identifies the rule.
state	<String>	Read-write	Enabled. Possible values = ENABLED, DISABLED
name	<String>	Read-write	Name of the profile to which to bind an exemption or rule. Minimum length = 1
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/appfwprofile_grpcvalidation_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"appfwprofile_grpcvalidation_binding":{

<b>"name":<String_value>,

</b>"comment":<String_value>,

"state":<String_value>,

"grpcvalidation":<String_value>,

"grpc_relax_validation_action":<String_value>,
```

```
"isautodeployed":<String_value>,

"resourceid":<String_value>,

"ruletype":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_grpcvalidation_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ appfwprofile_grpcvalidation_binding/ name_value<String> ? **args=grpcvalidation: <String_value> ,grpc_relax_validation_action: <String_value> ,ruletype: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_grpcvalidation_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ appfwprofile_grpcvalidation_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of appfwprofile_grpcvalidation_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_grpcvalidation_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the appfwprofile_grpcvalidation_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwprofile_grpcvalidation_binding": [ {

"alertonly":<String_value>,

"grpc_relax_validation_action":<String_value>,

"isautodeployed":<String_value>,

"comment":<String_value>,

"ruletype":<String_value>,

"grpcvalidation":<String_value>,

"resourceid":<String_value>,

"state":<String_value>,

"name":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_grpcvalidation_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_grpcvalidation_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwprofile_grpcvalidation_binding": [ {

"alertonly":<String_value>,

"grpc_relax_validation_action":<String_value>,

"isautodeployed":<String_value>,

"comment":<String_value>,

"ruletype":<String_value>,

"grpcvalidation":<String_value>,

"resourceid":<String_value>,
```

```
"state":<String_value>,

"name":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_grpcvalidation_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"appfwprofile_grpcvalidation_binding": [ { "__count": "#no"} ] }
```

appfwprofile_jsonblockkeyword_binding

Binding object showing the jsonblockkeyword that can be bound to appfwprofile.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
state	<String>	Read-write	Enabled.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ENABLED, DISABLED
keyname_json_blockkeyword	<String>	Read-write	JSON block keyword keyname.
resourceid	<String>	Read-write	A "id" that identifies the rule.
name	<String>	Read-write	Name of the profile to which to bind an exemption or rule. Minimum length = 1
jsonblockkeyword	<String>	Read-write	Field name of json block keyword binding.
comment	<String>	Read-write	Any comments about the purpose of profile, or other useful information about the profile.
ruletype	<String>	Read-write	Specifies rule type of binding. Possible values = ALLOW, DENY
iskeyregex_json_blockkeyword	<String>	Read-write	Is JSON blockkeyword key a regular expression?. Default value: NOTREGEX Possible values = REGEX, NOTREGEX

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
jsonblockkeywordtype	<String>	Read-write	JSON block keyword type. Possible values = literal, PCRE
jsonblockkeywordurl	<String>	Read-write	The json blockkeyword URL.
isautodeployed	<String>	Read-write	Is the rule auto deployed by dynamic profile ?. Possible values = AUTODEPLOYED, NOTAUTODEPLOYED
alertonly	<String>	Read-write	Send SNMP alert?. Possible values = ON, OFF
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/appfwprofile_jsonblockkeyword_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"appfwprofile_jsonblockkeyword_binding":{

<b>"name":<String_value>,

</b>"comment":<String_value>,

"state":<String_value>,

"isautodeployed":<String_value>,
```

```
"resourceid":<String_value>,

"jsonblockkeyword":<String_value>,

"keyname_json_blockkeyword":<String_value>,

"jsonblockkeywordurl":<String_value>,

"iskeyregex_json_blockkeyword":<String_value>,

"jsonblockkeywordtype":<String_value>,

"ruletype":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_jsonblockkeyword_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ appfwprofile_jsonblockkeyword_binding/ name_value<String> ? **args=jsonblockkeyword: <String_value> ,keyname_json_blockkeyword: <String_value> ,jsonblockkeywordurl: <String_value> ,ruletype: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_jsonblockkeyword_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ appfwprofile_jsonblockkeyword_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of appfwprofile_jsonblockkeyword_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_jsonblockkeyword_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the appfwprofile_jsonblockkeyword_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwprofile_jsonblockkeyword_binding": [ {

"state":<String_value>,

"keyname_json_blockkeyword":<String_value>,

"resourceid":<String_value>,

"name":<String_value>,

"jsonblockkeyword":<String_value>,
```

```
"comment":<String_value>,

"ruletype":<String_value>,

"iskeyregex_json_blockkeyword":<String_value>,

"jsonblockkeywordtype":<String_value>,

"jsonblockkeywordurl":<String_value>,

"isautodeployed":<String_value>,

"alertonly":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_jsonblockkeyword_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_jsonblockkeyword_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwprofile_jsonblockkeyword_binding": [ {

"state":<String_value>,

"keyname_json_blockkeyword":<String_value>,

"resourceid":<String_value>,

"name":<String_value>,

"jsonblockkeyword":<String_value>,

"comment":<String_value>,

"ruletype":<String_value>,

"iskeyregex_json_blockkeyword":<String_value>,

"jsonblockkeywordtype":<String_value>,

"jsonblockkeywordurl":<String_value>,

"isautodeployed":<String_value>,

"alertonly":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_jsonblockkeyword_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"appfwprofile_jsonblockkeyword_binding": [ { "__count": "#no"} ] }
```

appfwprofile_jsoncmdurl_binding

Binding object showing the jsoncmdurl that can be bound to appfwprofile.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
state	<String>	Read-write	Enabled. Possible values = ENABLED, DISABLED
resourceid	<String>	Read-write	A "id" that identifies the rule.
jsoncmdurl	<String>	Read-write	A regular expression that designates a URL on the Json CMD URL list for which Command injection violations are relaxed. Enclose URLs in double quotes to ensure preservation of any embedded spaces or non-alphanumeric characters.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum length = 1 Maximum length = 2047
name	<String>	Read-write	Name of the profile to which to bind an exemption or rule. Minimum length = 1
iskeyregex_json_cmd	<String>	Read-write	Is the key name a regular expression?. Possible values = REGEX, NOTREGEX
keyname_json_cmd	<String>	Read-write	An expression that designates a keyname on the JSON CMD URL for which Command injection violations are relaxed. Minimum length = 1
as_value_expr_json_cmd	<String>	Read-write	The JSON CMD key value expression.
isvalueregex_json_cmd	<String>	Read-write	Is the JSON CMD key value a regular expression?. Possible values = REGEX, NOTREGEX
isautodeployed	<String>	Read-write	Is the rule auto deployed by dynamic profile ?. Possible values = AUTODEPLOYED,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			NOTAUTODEPLOYED
alertonly	<String>	Read-write	Send SNMP alert?. Possible values = ON, OFF
comment	<String>	Read-write	Any comments about the purpose of profile, or other useful information about the profile.
ruletype	<String>	Read-write	Specifies rule type of binding. Possible values = ALLOW, DENY
as_value_type_json_cmd	<String>	Read-write	Type of the relaxed JSON CMD key value. Possible values = Keyword, SpecialString
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/appfwprofile_jsoncmdurl_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"appfwprofile_jsoncmdurl_binding":{

<b>"name":<String_value>,
```

```
</b>"comment":<String_value>,

"state":<String_value>,

"jsoncmdurl":<String_value>,

"keyname_json_cmd":<String_value>,

"iskeyregex_json_cmd":<String_value>,

"as_value_type_json_cmd":<String_value>,

"as_value_expr_json_cmd":<String_value>,

"isvalueregex_json_cmd":<String_value>,

"isautodeployed":<String_value>,

"resourceid":<String_value>,

"ruletype":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_jsoncmdurl_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ appfwprofile_jsoncmdurl_binding/ name_value<String> ? **args=jsoncmdurl: <String_value> ,keyname_json_cmd: <String_value> ,as_value_type_json_cmd: <String_value> ,as_value_expr_json_cmd: <String_value> ,ruletype: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_jsoncmdurl_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ appfwprofile_jsoncmdurl_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of appfwprofile_jsoncmdurl_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_jsoncmdurl_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the appfwprofile_jsoncmdurl_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwprofile_jsoncmdurl_binding": [ {

"state":<String_value>,

"resourceid":<String_value>,
```

```
"jsoncmdurl":<String_value>,

"name":<String_value>,

"iskeyregex_json_cmd":<String_value>,

"keyname_json_cmd":<String_value>,

"as_value_expr_json_cmd":<String_value>,

"isvalueregex_json_cmd":<String_value>,

"isautodeployed":<String_value>,

"alertonly":<String_value>,

"comment":<String_value>,

"ruletype":<String_value>,

"as_value_type_json_cmd":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_jsoncmdurl_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_jsoncmdurl_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwprofile_jsoncmdurl_binding": [ {

"state":<String_value>,

"resourceid":<String_value>,

"jsoncmdurl":<String_value>,

"name":<String_value>,

"iskeyregex_json_cmd":<String_value>,

"keyname_json_cmd":<String_value>,

"as_value_expr_json_cmd":<String_value>,

"isvalueregex_json_cmd":<String_value>,

"isautodeployed":<String_value>,

"alertonly":<String_value>,

"comment":<String_value>,

"ruletype":<String_value>,

"as_value_type_json_cmd":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_jsoncmdurl_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"appfwprofile_jsoncmdurl_binding": [ { "__count": "#no"} ] }
```

appfwprofile_jsondosurl_binding

Binding object showing the jsondosurl that can be bound to appfwprofile.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
jsonmaxstringlengthcheck	<String>	Read-write	State if JSON Max string value count check is ON or OFF. Possible values = ON, OFF
jsonmaxobjectkeylengthcheck	<String>	Read-write	State if JSON Max object key length check is ON or OFF. Possible values = ON, OFF
jsonmaxstringlength	<Integer>	Read-write	Maximum string length in the JSON.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			This check protects against strings that have large length. Default value: 1000000 Minimum value = 0 Maximum value = 2147483647
isautodeployed	<String>	Read-write	Is the rule auto deployed by dynamic profile ?. Possible values = AUTODEPLOYED, NOTAUTODEPLOYED
alertonly	<String>	Read-write	Send SNMP alert?. Possible values = ON, OFF
jsonmaxcontainerdepth	<Integer>	Read-write	Maximum allowed nesting depth of JSON document. JSON allows one to nest the containers (object and array) in any order to any depth. This check protects against documents that have excessive depth of hierarchy. Default value: 5 Minimum value = 0

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum value = 127
jsonmaxobjectkeycountcheck	<String>	Read-write	State if JSON Max object key count check is ON or OFF. Possible values = ON, OFF
comment	<String>	Read-write	Any comments about the purpose of profile, or other useful information about the profile.
jsonmaxarraylengthcheck	<String>	Read-write	State if JSON Max array value count check is ON or OFF. Possible values = ON, OFF
ruletype	<String>	Read-write	Specifies rule type of binding. Possible values = ALLOW, DENY
jsondosurl	<String>	Read-write	The URL on which we need to enforce the specified JSON denial-of-service (JSONDoS) attack protections. An JSON DoS configuration consists of the following items: * URL. PCRE-format regular expression for the URL. * Maximum-document-

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			length-check toggle. ON to enable this check, OFF to disable it. * Maximum document length. Positive integer representing the maximum length of the JSON document. * Maximum-container-depth-check toggle. ON to enable, OFF to disable. * Maximum container depth. Positive integer representing the maximum container depth of the JSON document. * Maximum-object-key-count-check toggle. ON to enable, OFF to disable. * Maximum object key count. Positive integer representing the maximum allowed number of keys in any of the JSON object. * Maximum-object-key-length-check toggle. ON to enable, OFF to disable. * Maximum object key length. Positive integer representing the maximum allowed length of key in any of the JSON

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			object. * Maximum-array-value-count-check toggle. ON to enable, OFF to disable. * Maximum array value count. Positive integer representing the maximum allowed number of values in any of the JSON array. * Maximum-string-length-check toggle. ON to enable, OFF to disable. * Maximum string length. Positive integer representing the maximum length of string in JSON. Minimum length = 1 Maximum length = 2047
jsonmaxdocumentlengthcheck	<String>	Read-write	State if JSON Max document length check is ON or OFF. Possible values = ON, OFF
jsonmaxobjectkeycount	<Integer>	Read-write	Maximum key count in the any of JSON object. This check protects against objects that have large number of keys.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: 10000 Minimum value = 0 Maximum value = 2147483647
jsonmaxobjectkeylength	<Integer>	Read-write	Maximum key length in the any of JSON object. This check protects against objects that have large keys. Default value: 128 Minimum value = 0 Maximum value = 2147483647
state	<String>	Read-write	Enabled. Possible values = ENABLED, DISABLED
jsonmaxcontainerdepthcheck	<String>	Read-write	State if JSON Max depth check is ON or OFF. Possible values = ON, OFF
jsonmaxarraylength	<Integer>	Read-write	Maximum array length in the any of JSON object. This check protects against arrays having large lengths.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: 10000 Minimum value = 0 Maximum value = 2147483647
resourceid	<String>	Read-write	A "id" that identifies the rule.
name	<String>	Read-write	Name of the profile to which to bind an exemption or rule. Minimum length = 1
jsonmaxdocumentlength	<Integer>	Read-write	Maximum document length of JSON document, in bytes. Default value: 20000000 Minimum value = 0 Maximum value = 2147483647
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/appfwprofile_jsondosurl_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"appfwprofile_jsondosurl_binding":{

<b>"name":<String_value>,
```

```
</b>"comment":<String_value>,

"state":<String_value>,

"jsondosurl":<String_value>,

"jsonmaxcontainerdepthcheck":<String_value>,

"jsonmaxcontainerdepth":<Integer_value>,

"jsonmaxdocumentlengthcheck":<String_value>,

"jsonmaxdocumentlength":<Integer_value>,

"jsonmaxobjectkeycountcheck":<String_value>,

"jsonmaxobjectkeycount":<Integer_value>,

"jsonmaxobjectkeylengthcheck":<String_value>,

"jsonmaxobjectkeylength":<Integer_value>,

"jsonmaxarraylengthcheck":<String_value>,

"jsonmaxarraylength":<Integer_value>,

"jsonmaxstringlengthcheck":<String_value>,

"jsonmaxstringlength":<Integer_value>,

"isautodeployed":<String_value>,

"resourceid":<String_value>,

"ruletype":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_jsondosurl_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ appfwprofile_jsondosurl_binding/ name_value<String> ? **args=jsondosurl: <String_value> ,ruletype: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_jsondosurl_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ appfwprofile_jsondosurl_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of appfwprofile_jsondosurl_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_jsondosurl_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the appfwprofile_jsondosurl_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwprofile_jsondosurl_binding": [ {

"jsonmaxstringlengthcheck":<String_value>,

"jsonmaxobjectkeylengthcheck":<String_value>,

"jsonmaxstringlength":<Integer_value>,

"isautodeployed":<String_value>,

"alertonly":<String_value>,

"jsonmaxcontainerdepth":<Integer_value>,

"jsonmaxobjectkeycountcheck":<String_value>,

"comment":<String_value>,

"jsonmaxarraylengthcheck":<String_value>,

"ruletype":<String_value>,

"jsondosurl":<String_value>,

"jsonmaxdocumentlengthcheck":<String_value>,

"jsonmaxobjectkeycount":<Integer_value>,

"jsonmaxobjectkeylength":<Integer_value>,

"state":<String_value>,

"jsonmaxcontainerdepthcheck":<String_value>,
```

```
"jsonmaxarraylength":<Integer_value>,

"resourceid":<String_value>,

"name":<String_value>,

"jsonmaxdocumentlength":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_jsondosurl_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_jsondosurl_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwprofile_jsondosurl_binding": [ {

"jsonmaxstringlengthcheck":<String_value>,
```

```
"jsonmaxobjectkeylengthcheck":<String_value>,

"jsonmaxstringlength":<Integer_value>,

"isautodeployed":<String_value>,

"alertonly":<String_value>,

"jsonmaxcontainerdepth":<Integer_value>,

"jsonmaxobjectkeycountcheck":<String_value>,

"comment":<String_value>,

"jsonmaxarraylengthcheck":<String_value>,

"ruletype":<String_value>,

"jsondosurl":<String_value>,

"jsonmaxdocumentlengthcheck":<String_value>,

"jsonmaxobjectkeycount":<Integer_value>,

"jsonmaxobjectkeylength":<Integer_value>,

"state":<String_value>,

"jsonmaxcontainerdepthcheck":<String_value>,

"jsonmaxarraylength":<Integer_value>,

"resourceid":<String_value>,

"name":<String_value>,

"jsonmaxdocumentlength":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_jsondosurl_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"appfwprofile_jsondosurl_binding": [ { "__count": "#no"} ] }
```

appfwprofile_jsonsqlurl_binding

Binding object showing the jsonsqlurl that can be bound to appfwprofile.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the profile to which to bind an exemption or rule. Minimum length = 1
resourceid	<String>	Read-write	A "id" that identifies the rule.
state	<String>	Read-write	Enabled.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ENABLED, DISABLED
iskeyregex_json_sql	<String>	Read-write	Is the key name a regular expression?. Possible values = REGEX, NOTREGEX
isvalueregex_json_sql	<String>	Read-write	Is the JSON SQL key value a regular expression?. Possible values = REGEX, NOTREGEX
jsonsqlurl	<String>	Read-write	A regular expression that designates a URL on the Json SQL URL list for which SQL violations are relaxed. Enclose URLs in double quotes to ensure preservation of any embedded spaces or non-alphanumeric characters. Minimum length = 1 Maximum length = 2047
ruletype	<String>	Read-write	Specifies rule type of binding. Possible values = ALLOW, DENY

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
comment	<String>	Read-write	Any comments about the purpose of profile, or other useful information about the profile.
as_value_expr_json_sql	<String>	Read-write	The JSON SQL key value expression.
keyname_json_sql	<String>	Read-write	An expression that designates a keyname on the JSON SQL URL for which SQL injection violations are relaxed. Minimum length = 1
alertonly	<String>	Read-write	Send SNMP alert?. Possible values = ON, OFF
as_value_type_json_sql	<String>	Read-write	Type of the relaxed JSON SQL key value. Possible values = Keyword, SpecialString, Wildchar
isautodeployed	<String>	Read-write	Is the rule auto deployed by dynamic profile ?. Possible values = AUTODEPLOYED, NOTAUTODEPLOYED
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/appfwprofile_jsonsqlurl_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"appfwprofile_jsonsqlurl_binding":{

<b>"name":<String_value>,

</b>"comment":<String_value>,

"state":<String_value>,

"jsonsqlurl":<String_value>,

"keyname_json_sql":<String_value>,

"iskeyregex_json_sql":<String_value>,

"as_value_type_json_sql":<String_value>,

"as_value_expr_json_sql":<String_value>,

"isvalueregex_json_sql":<String_value>,

"isautodeployed":<String_value>,

"resourceid":<String_value>,

"ruletype":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_jsonsqlurl_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ appfwprofile_jsonsqlurl_binding/ name_value<String> ? **args=jsonsqlurl: <String_value> ,keyname_json_sql: <String_value> ,as_value_type_json_sql: <String_value> ,as_value_expr_json_sql: <String_value> ,ruletype: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_jsonsqlurl_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ appfwprofile_jsonsqlurl_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of appfwprofile_jsonsqlurl_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_jsonsqlurl_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the appfwprofile_jsonsqlurl_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwprofile_jsonsqlurl_binding": [ {

"name":<String_value>,

"resourceid":<String_value>,

"state":<String_value>,

"iskeyregex_json_sql":<String_value>,

"isvalueregex_json_sql":<String_value>,

"jsonsqlurl":<String_value>,

"ruletype":<String_value>,

"comment":<String_value>,

"as_value_expr_json_sql":<String_value>,

"keyname_json_sql":<String_value>,

"alertonly":<String_value>,

"as_value_type_json_sql":<String_value>,

"isautodeployed":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_jsonsqlurl_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_jsonsqlurl_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwprofile_jsonsqlurl_binding": [ {

"name":<String_value>,

"resourceid":<String_value>,

"state":<String_value>,

"iskeyregex_json_sql":<String_value>,

"isvalueregex_json_sql":<String_value>,

"jsonsqlurl":<String_value>,

"ruletype":<String_value>,

"comment":<String_value>,

"as_value_expr_json_sql":<String_value>,

"keyname_json_sql":<String_value>,
```

```
"alertonly":<String_value>,

"as_value_type_json_sql":<String_value>,

"isautodeployed":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_jsonsqlurl_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"appfwprofile_jsonsqlurl_binding": [ { "__count": "#no"} ] }
```

appfwprofile_jsonxssurl_binding

Binding object showing the jsonxssurl that can be bound to appfwprofile.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the profile to which to bind an exemption or rule. Minimum length = 1
keyname_json_xss	<String>	Read-write	An expression that designates a keyname on the JSON XSS URL for which XSS injection violations are relaxed. Minimum length = 1
state	<String>	Read-write	Enabled. Possible values = ENABLED, DISABLED
resourceid	<String>	Read-write	A "id" that identifies the rule.
iskeyregex_json_xss	<String>	Read-write	Is the key name a regular expression?. Possible values = REGEX, NOTREGEX
jsonxssurl	<String>	Read-write	A regular expression that designates a URL on the Json XSS URL list for which XSS violations are relaxed. Enclose URLs in double quotes to ensure preservation of any embedded spaces or

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			non-alphanumeric characters. Minimum length = 1 Maximum length = 2047
ruletype	<String>	Read-write	Specifies rule type of binding. Possible values = ALLOW, DENY
as_value_expr_json_xss	<String>	Read-write	The JSON XSS key value expression.
comment	<String>	Read-write	Any comments about the purpose of profile, or other useful information about the profile.
isautodeployed	<String>	Read-write	Is the rule auto deployed by dynamic profile ?. Possible values = AUTODEPLOYED, NOTAUTODEPLOYED
alertonly	<String>	Read-write	Send SNMP alert?. Possible values = ON, OFF
isvalueregex_json_xss	<String>	Read-write	Is the JSON XSS key value a regular expression?. Possible values = REGEX, NOTREGEX

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
as_value_type_json_xss	<String>	Read-write	Type of the relaxed JSON XSS key value. Possible values = Tag, Attribute, Pattern
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/appfwprofile_jsonxssurl_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"appfwprofile_jsonxssurl_binding":{

<b>"name":<String_value>,

</b>"comment":<String_value>,

"state":<String_value>,

"jsonxssurl":<String_value>,

"keyname_json_xss":<String_value>,

"iskeyregex_json_xss":<String_value>,

"as_value_type_json_xss":<String_value>,

"as_value_expr_json_xss":<String_value>,

"isvalueregex_json_xss":<String_value>,

"isautodeployed":<String_value>,
```

```
"resourceid":<String_value>,

"ruletype":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_jsonxssurl_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ appfwprofile_jsonxssurl_binding/ name_value<String> ? **args=jsonxssurl: <String_value> ,keyname_json_xss: <String_value> ,as_value_type_json_xss: <String_value> ,as_value_expr_json_xss: <String_value> ,ruletype: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_jsonxssurl_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ appfwprofile_jsonxssurl_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of appfwprofile_jsonxssurl_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_jsonxssurl_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the appfwprofile_jsonxssurl_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwprofile_jsonxssurl_binding": [ {

"name":<String_value>,

"keyname_json_xss":<String_value>,

"state":<String_value>,

"resourceid":<String_value>,

"iskeyregex_json_xss":<String_value>,

"jsonxssurl":<String_value>,

"ruletype":<String_value>,

"as_value_expr_json_xss":<String_value>,

"comment":<String_value>,

"isautodeployed":<String_value>,

"alertonly":<String_value>,
```

```
"isvalueregex_json_xss":<String_value>,

"as_value_type_json_xss":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_jsonxssurl_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_jsonxssurl_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwprofile_jsonxssurl_binding": [ {

"name":<String_value>,

"keyname_json_xss":<String_value>,

"state":<String_value>,
```

```
"resourceid":<String_value>,

"iskeyregex_json_xss":<String_value>,

"jsonxssurl":<String_value>,

"ruletype":<String_value>,

"as_value_expr_json_xss":<String_value>,

"comment":<String_value>,

"isautodeployed":<String_value>,

"alertonly":<String_value>,

"isvalueregex_json_xss":<String_value>,

"as_value_type_json_xss":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_jsonxssurl_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"appfwprofile_jsonxssurl_binding": [ { "__count": "#no"} ] }
```

appfwprofile_logexpression_binding

Binding object showing the logexpression that can be bound to appfwprofile.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
as_logexpression	<String>	Read-write	LogExpression to log when violation happened on appfw profile. Maximum length = 1500
name	<String>	Read-write	Name of the profile to which to bind an exemption or rule. Minimum length = 1
resourceid	<String>	Read-write	A "id" that identifies the rule.
state	<String>	Read-write	Enabled. Possible values = ENABLED, DISABLED
alertonly	<String>	Read-write	Send SNMP alert?. Possible values = ON, OFF
isautodeployed	<String>	Read-write	Is the rule auto deployed by dynamic profile ?. Possible values = AUTODEPLOYED,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			NOTAUTODEPLOYED
logexpression	<String>	Read-write	Name of LogExpression object.
ruletype	<String>	Read-write	Specifies rule type of binding. Possible values = ALLOW, DENY
comment	<String>	Read-write	Any comments about the purpose of profile, or other useful information about the profile.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/appfwprofile_logexpression_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"appfwprofile_logexpression_binding":{

<b>"name":<String_value>,

</b>"comment":<String_value>,

"state":<String_value>,

"logexpression":<String_value>,

"as_logexpression":<String_value>,
```

```
"isautodeployed":<String_value>,

"resourceid":<String_value>,

"ruletype":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_logexpression_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ appfwprofile_logexpression_binding/ name_value<String> ? **args=logexpression: <String_value> ,ruletype: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_logexpression_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ appfwprofile_logexpression_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of appfwprofile_logexpression_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_logexpression_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the appfwprofile_logexpression_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwprofile_logexpression_binding": [ {

"as_logexpression":<String_value>,

"name":<String_value>,

"resourceid":<String_value>,

"state":<String_value>,

"alertonly":<String_value>,

"isautodeployed":<String_value>,

"logexpression":<String_value>,

"ruletype":<String_value>,

"comment":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_logexpression_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_logexpression_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwprofile_logexpression_binding": [ {

"as_logexpression":<String_value>,

"name":<String_value>,

"resourceid":<String_value>,

"state":<String_value>,

"alertonly":<String_value>,

"isautodeployed":<String_value>,

"logexpression":<String_value>,
```

```
"ruletype":<String_value>,

"comment":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_logexpression_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"appfwprofile_logexpression_binding": [ { "__count": "#no"} ] }
```

appfwprofile_restvalidation_binding

Binding object showing the restvalidation that can be bound to appfwprofile.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
comment	<String>	Read-write	Any comments about the purpose of

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			profile, or other useful information about the profile.
state	<String>	Read-write	Enabled. Possible values = ENABLED, DISABLED
resourceid	<String>	Read-write	A "id" that identifies the rule.
ruletype	<String>	Read-write	Specifies rule type of binding. Possible values = ALLOW, DENY
isautodeployed	<String>	Read-write	Is the rule auto deployed by dynamic profile ?. Possible values = AUTODEPLOYED, NOTAUTODEPLOYED
name	<String>	Read-write	Name of the profile to which to bind an exemption or rule. Minimum length = 1
alertonly	<String>	Read-write	Send SNMP alert?. Possible values = ON, OFF
restvalidation	<String>	Read-write	Exempt REST endpoints or any other URLs matching the given pattern from the API schema validation check.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Example: GET:/v1/bookstore/viewbooks.
rest_validation_action	<String>	Read-write	Action to be taken for traffic matching the configured relaxation rule. Default value: none Possible values = log, none
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/appfwprofile_restvalidation_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"appfwprofile_restvalidation_binding":{

<b>"name":<String_value>,

</b>"comment":<String_value>,

"state":<String_value>,

"restvalidation":<String_value>,

"rest_validation_action":<String_value>,

"isautodeployed":<String_value>,

"resourceid":<String_value>,

"ruletype":<String_value>
```

```
}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_restvalidation_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ appfwprofile_restvalidation_binding/ name_value<String> ? **args=restvalidation: <String_value> ,rest_validation_action: <String_value> ,ruletype: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_restvalidation_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ appfwprofile_restvalidation_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of appfwprofile_restvalidation_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_restvalidation_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the appfwprofile_restvalidation_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwprofile_restvalidation_binding": [ {

"comment":<String_value>,

"state":<String_value>,

"resourceid":<String_value>,

"ruletype":<String_value>,

"isautodeployed":<String_value>,

"name":<String_value>,

"alertonly":<String_value>,

"restvalidation":<String_value>,

"rest_validation_action":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_restvalidation_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_restvalidation_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwprofile_restvalidation_binding": [ {

"comment":<String_value>,

"state":<String_value>,

"resourceid":<String_value>,

"ruletype":<String_value>,

"isautodeployed":<String_value>,

"name":<String_value>,

"alertonly":<String_value>,

"restvalidation":<String_value>,

"rest_validation_action":<String_value>

}]}
```

```
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_restvalidation_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"appfwprofile_restvalidation_binding": [ { "__count": "#no"} ] }
```

appfwprofile_safeobject_binding

Binding object showing the safeobject that can be bound to appfwprofile.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
state	<String>	Read-write	Enabled. Possible values = ENABLED, DISABLED
comment	<String>	Read-write	Any comments about the purpose of profile, or other

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			useful information about the profile.
action	<String[]>	Read-write	Safe Object action types. (BLOCK | LOG | STATS | NONE). Possible values = none, block, log, remove, stats, xout
resourceid	<String>	Read-write	A "id" that identifies the rule.
maxmatchlength	<Integer>	Read-write	Maximum match length for a Safe Object expression.
safeobject	<String>	Read-write	Name of the Safe Object.
as_expression	<String>	Read-write	A regular expression that defines the Safe Object.
ruletype	<String>	Read-write	Specifies rule type of binding. Possible values = ALLOW, DENY
isautodeployed	<String>	Read-write	Is the rule auto deployed by dynamic profile ?. Possible values = AUTODEPLOYED, NOTAUTODEPLOYED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the profile to which to bind an exemption or rule. Minimum length = 1
alertonly	<String>	Read-write	Send SNMP alert?. Possible values = ON, OFF
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/appfwprofile_safeobject_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"appfwprofile_safeobject_binding":{

<b>"name":<String_value>,

</b>"safeobject":<String_value>,

"as_expression":<String_value>,

"maxmatchlength":<Integer_value>,

"action":<String[]_value>,

"comment":<String_value>,

"state":<String_value>,

"isautodeployed":<String_value>,

"resourceid":<String_value>,
```

```
"ruletype":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_safeobject_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ appfwprofile_safeobject_binding/ name_value<String> ? **args=safeobject: <String_value> ,ruletype: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_safeobject_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ appfwprofile_safeobject_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of appfwprofile_safeobject_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_safeobject_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the appfwprofile_safeobject_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwprofile_safeobject_binding": [ {

"state":<String_value>,

"comment":<String_value>,

"action":<String[]_value>,

"resourceid":<String_value>,

"maxmatchlength":<Integer_value>,

"safeobject":<String_value>,

"as_expression":<String_value>,

"ruletype":<String_value>,

"isautodeployed":<String_value>,

"name":<String_value>,

"alertonly":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_safeobject_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_safeobject_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwprofile_safeobject_binding": [ {

"state":<String_value>,

"comment":<String_value>,

"action":<String[]_value>,

"resourceid":<String_value>,

"maxmatchlength":<Integer_value>,

"safeobject":<String_value>,

"as_expression":<String_value>,
```

```
"ruletype":<String_value>,

"isautodeployed":<String_value>,

"name":<String_value>,

"alertonly":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_safeobject_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"appfwprofile_safeobject_binding": [ { "__count": "#no"} ] }
```

appfwprofile_sqlinjection_binding

Binding object showing the sqlinjection that can be bound to appfwprofile.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
isvalueregex_sql	<String>	Read-write	Is the web form field value a regular expression?. Possible values = REGEX, NOTREGEX
alertonly	<String>	Read-write	Send SNMP alert?. Possible values = ON, OFF
formactionurl_sql	<String>	Read-write	The web form action URL.
as_value_type_sql	<String>	Read-write	The web form value type. Possible values = Keyword, SpecialString, Wildchar
name	<String>	Read-write	Name of the profile to which to bind an exemption or rule. Minimum length = 1
isautodeployed	<String>	Read-write	Is the rule auto deployed by dynamic profile ?. Possible values = AUTODEPLOYED, NOTAUTODEPLOYED
ruletype	<String>	Read-write	Specifies rule type of binding. Possible values = ALLOW, DENY

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
as_scan_location_sql	<String>	Read-write	Location of SQL injection exception - form field, header or cookie. Possible values = FORMFIELD, HEADER, COOKIE
resourceid	<String>	Read-write	A "id" that identifies the rule.
sqlinjection	<String>	Read-write	The web form field name.
as_value_expr_sql	<String>	Read-write	The web form value expression.
comment	<String>	Read-write	Any comments about the purpose of profile, or other useful information about the profile.
state	<String>	Read-write	Enabled. Possible values = ENABLED, DISABLED
isregex_sql	<String>	Read-write	Is the web form field name a regular expression?. Possible values = REGEX, NOTREGEX
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/appfwprofile_sqlinjection_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"appfwprofile_sqlinjection_binding":{

<b>"name":<String_value>,

</b>"sqlinjection":<String_value>,

"formactionurl_sql":<String_value>,

"isregex_sql":<String_value>,

"as_scan_location_sql":<String_value>,

"as_value_type_sql":<String_value>,

"as_value_expr_sql":<String_value>,

"isvalueregex_sql":<String_value>,

"comment":<String_value>,

"state":<String_value>,

"isautodeployed":<String_value>,

"resourceid":<String_value>,

"ruletype":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_sqlinjection_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ appfwprofile_sqlinjection_binding/ name_value<String> ? **args=sqlinjection: <String_value> ,formactionurl_sql: <String_value> ,as_scan_location_sql: <String_value> ,as_value_type_sql: <String_value> ,as_value_expr_sql: <String_value> ,ruletype: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_sqlinjection_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ appfwprofile_sqlinjection_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of appfwprofile_sqlinjection_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_sqlinjection_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the appfwprofile_sqlinjection_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwprofile_sqlinjection_binding": [ {

"isvalueregex_sql":<String_value>,

"alertonly":<String_value>,

"formactionurl_sql":<String_value>,

"as_value_type_sql":<String_value>,

"name":<String_value>,

"isautodeployed":<String_value>,

"ruletype":<String_value>,

"as_scan_location_sql":<String_value>,

"resourceid":<String_value>,

"sqlinjection":<String_value>,

"as_value_expr_sql":<String_value>,

"comment":<String_value>,

"state":<String_value>,

"isregex_sql":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_sqlinjection_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_sqlinjection_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwprofile_sqlinjection_binding": [ {

"isvalueregex_sql":<String_value>,

"alertonly":<String_value>,

"formactionurl_sql":<String_value>,

"as_value_type_sql":<String_value>,

"name":<String_value>,

"isautodeployed":<String_value>,

"ruletype":<String_value>,
```

```
"as_scan_location_sql":<String_value>,

"resourceid":<String_value>,

"sqlinjection":<String_value>,

"as_value_expr_sql":<String_value>,

"comment":<String_value>,

"state":<String_value>,

"isregex_sql":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_sqlinjection_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"appfwprofile_sqlinjection_binding": [ { "__count": "#no"} ] }
```

appfwprofile_starturl_binding

Binding object showing the starturl that can be bound to appfwprofile.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the profile to which to bind an exemption or rule. Minimum length = 1
state	<String>	Read-write	Enabled. Possible values = ENABLED, DISABLED
resourceid	<String>	Read-write	A "id" that identifies the rule.
isautodeployed	<String>	Read-write	Is the rule auto deployed by dynamic profile ?. Possible values = AUTODEPLOYED, NOTAUTODEPLOYED
alertonly	<String>	Read-write	Send SNMP alert?. Possible values = ON, OFF
ruletype	<String>	Read-write	Specifies rule type of binding. Possible values = ALLOW, DENY
starturl	<String>	Read-write	A regular expression that designates a

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			URL on the Start URL list.
comment	<String>	Read-write	Any comments about the purpose of profile, or other useful information about the profile.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/appfwprofile_starturl_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"appfwprofile_starturl_binding":{

<b>"name":<String_value>,

</b>"starturl":<String_value>,

"comment":<String_value>,

"state":<String_value>,

"isautodeployed":<String_value>,

"resourceid":<String_value>,

"ruletype":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_starturl_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ appfwprofile_starturl_binding/ name_value<String> ? **args=starturl: <String_value> ,ruletype: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_starturl_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ appfwprofile_starturl_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of appfwprofile_starturl_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_starturl_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the appfwprofile_starturl_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwprofile_starturl_binding": [ {

"name":<String_value>,

"state":<String_value>,

"resourceid":<String_value>,

"isautodeployed":<String_value>,

"alertonly":<String_value>,

"ruletype":<String_value>,

"starturl":<String_value>,

"comment":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_starturl_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_starturl_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwprofile_starturl_binding": [ {

"name":<String_value>,

"state":<String_value>,

"resourceid":<String_value>,

"isautodeployed":<String_value>,

"alertonly":<String_value>,

"ruletype":<String_value>,

"starturl":<String_value>,

"comment":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_starturl_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"appfwprofile_starturl_binding": [ { "__count": "#no"} ] }
```

appfwprofile_trustedlearningclients_binding

Binding object showing the trustedlearningclients that can be bound to appfwprofile.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
isautodeployed	<String>	Read-write	Is the rule auto deployed by dynamic profile ?. Possible values = AUTODEPLOYED, NOTAUTODEPLOYED
alertonly	<String>	Read-write	Send SNMP alert?. Possible values = ON, OFF
ruletype	<String>	Read-write	Specifies rule type of binding. Possible values = ALLOW, DENY

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
comment	<String>	Read-write	Any comments about the purpose of profile, or other useful information about the profile.
trustedlearningclients	<String>	Read-write	Specify trusted host/ network IP.
name	<String>	Read-write	Name of the profile to which to bind an exemption or rule. Minimum length = 1
state	<String>	Read-write	Enabled. Possible values = ENABLED, DISABLED
resourceid	<String>	Read-write	A "id" that identifies the rule.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/appfwprofile_trustedlearningclients_binding
HTTP Method: PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"appfwprofile_trustedlearningclients_binding":{

<b>"name":<String_value>,

</b>"trustedlearningclients":<String_value>,

"comment":<String_value>,
```

```
"state":<String_value>,

"isautodeployed":<String_value>,

"resourceid":<String_value>,

"ruletype":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_trustedlearningclients_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ appfwprofile_trustedlearningclients_binding/ name_value<String> ? **args=trustedlearningclients: <String_value> ,ruletype: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_trustedlearningclients_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ appfwprofile_trustedlearningclients_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of appfwprofile_trustedlearningclients_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ appfwprofile_trustedlearningclients_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the appfwprofile_trustedlearningclients_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwprofile_trustedlearningclients_binding": [ {

"isautodeployed":<String_value>,

"alertonly":<String_value>,

"ruletype":<String_value>,

"comment":<String_value>,

"trustedlearningclients":<String_value>,

"name":<String_value>,

"state":<String_value>,

"resourceid":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_trustedlearningclients_binding
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_trustedlearningclients_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwprofile_trustedlearningclients_binding": [ {

"isautodeployed":<String_value>,

"alertonly":<String_value>,

"ruletype":<String_value>,

"comment":<String_value>,

"trustedlearningclients":<String_value>,

"name":<String_value>,
```

```
"state":<String_value>,

"resourceid":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_trustedlearningclients_binding/name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"appfwprofile_trustedlearningclients_binding": [ { "__count": "#no"} ] }
```

appfwprofile_xmlattachmenturl_binding

Binding object showing the xmlattachmenturl that can be bound to appfwprofile.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
xmlattachmenturl	<String>	Read-write	XML attachment URL regular expression length.
alertonly	<String>	Read-write	Send SNMP alert?. Possible values = ON, OFF
xmlattachmentcontenttype	<String>	Read-write	Specify content-type regular expression.
name	<String>	Read-write	Name of the profile to which to bind an exemption or rule. Minimum length = 1
isautodeployed	<String>	Read-write	Is the rule auto deployed by dynamic profile ?. Possible values = AUTODEPLOYED, NOTAUTODEPLOYED
xmlattachmentcontenttypecheck	<String>	Read-write	State if XML attachment content-type check is ON or OFF. Protects against XML requests with illegal attachments. Possible values = ON, OFF
xmlmaxattachmentsize	<Integer>	Read-write	Specify maximum attachment size. Minimum value = 0

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum value = 1000000000
ruletype	<String>	Read-write	Specifies rule type of binding. Possible values = ALLOW, DENY
xmlmaxattachmentsizecheck	<String>	Read-write	State if XML Max attachment size Check is ON or OFF. Protects against XML requests with large attachment data. Possible values = ON, OFF
resourceid	<String>	Read-write	A "id" that identifies the rule.
comment	<String>	Read-write	Any comments about the purpose of profile, or other useful information about the profile.
state	<String>	Read-write	Enabled. Possible values = ENABLED, DISABLED
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/appfwprofile_xmlattachmenturl_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"appfwprofile_xmlattachmenturl_binding":{

<b>"name":<String_value>,

</b>"comment":<String_value>,

"state":<String_value>,

"xmlattachmenturl":<String_value>,

"xmlmaxattachmentsizecheck":<String_value>,

"xmlmaxattachmentsize":<Integer_value>,

"xmlattachmentcontenttypecheck":<String_value>,

"xmlattachmentcontenttype":<String_value>,

"isautodeployed":<String_value>,

"resourceid":<String_value>,

"ruletype":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_xmlattachmenturl_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ appfwprofile_xmlattachmenturl_binding/ name_value<String> ? **args=xmlattachmenturl: <String_value> ,ruletype: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_xmlattachmenturl_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ appfwprofile_xmlattachmenturl_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of appfwprofile_xmlattachmenturl_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_xmlattachmenturl_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the appfwprofile_xmlattachmenturl_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwprofile_xmlattachmenturl_binding": [ {

"xmlattachmenturl":<String_value>,

"alertonly":<String_value>,

"xmlattachmentcontenttype":<String_value>,

"name":<String_value>,

"isautodeployed":<String_value>,

"xmlattachmentcontenttypecheck":<String_value>,

"xmlmaxattachmentsize":<Integer_value>,

"ruletype":<String_value>,

"xmlmaxattachmentsizecheck":<String_value>,

"resourceid":<String_value>,

"comment":<String_value>,

"state":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_xmlattachmenturl_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_xmlattachmenturl_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwprofile_xmlattachmenturl_binding": [ {

"xmlattachmenturl":<String_value>,

"alertonly":<String_value>,

"xmlattachmentcontenttype":<String_value>,

"name":<String_value>,

"isautodeployed":<String_value>,

"xmlattachmentcontenttypecheck":<String_value>,

"xmlmaxattachmentsize":<Integer_value>,

"ruletype":<String_value>,

"xmlmaxattachmentsizecheck":<String_value>,

"resourceid":<String_value>,

"comment":<String_value>,

"state":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_xmlattachmenturl_binding/name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"appfwprofile_xmlattachmenturl_binding": [ { "__count": "#no"} ] }
```

appfwprofile_xmldosurl_binding

Binding object showing the xmldosurl that can be bound to appfwprofile.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
xmlmaxentityexpansiondepth	<Integer>	Read-write	Specify maximum entity expansion depth. Protects aganist Entity Expansion Attack.
xmlmaxattributenamelengthcheck	<String>	Read-write	State if XML Max attribute name length check is ON or OFF.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ON, OFF
xmlmaxattributenamelength	<Integer>	Read-write	Specify the longest name of any XML attribute. Protects against overflow attacks.
xmlmaxelementnamelengthcheck	<String>	Read-write	State if XML Max element name length check is ON or OFF. Possible values = ON, OFF
xmlmaxelements	<Integer>	Read-write	Specify the maximum number of XML elements allowed. Protects against overflow attacks.
state	<String>	Read-write	Enabled. Possible values = ENABLED, DISABLED
xmlmaxattributevaluelengthcheck	<String>	Read-write	State if XML Max atribute value length is ON or OFF. Possible values = ON, OFF
xmlmaxattributevaluelength	<Integer>	Read-write	Specify the longest value of any XML attribute. Protects against overflow attacks.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
xmlminfilesizecheck	<String>	Read-write	State if XML Min file size check is ON or OFF. Possible values = ON, OFF
resourceid	<String>	Read-write	A "id" that identifies the rule.
xmlmaxfilesize	<Integer>	Read-write	Specify the maximum size of XML messages. Protects against overflow attacks. Minimum value = 0 Maximum value = 1000000000
xmlmaxelementchildren	<Integer>	Read-write	Specify the maximum number of children allowed per XML element. Protects against overflow attacks.
xmlmaxsoaparrayrank	<Integer>	Read-write	XML Max Individual SOAP Array Rank. This is the dimension of the SOAP array.
name	<String>	Read-write	Name of the profile to which to bind an exemption or rule. Minimum length = 1
xmlsoaparraycheck	<String>	Read-write	State if XML SOAP Array check is ON or OFF.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ON, OFF
xmlmaxelementchildrencheck	<String>	Read-write	State if XML Max element children check is ON or OFF. Possible values = ON, OFF
xmlmaxnodes	<Integer>	Read-write	Specify the maximum number of XML nodes. Protects against overflow attacks.
xmlmaxelementdepth	<Integer>	Read-write	Maximum nesting (depth) of XML elements. This check protects against documents that have excessive hierarchy depths.
xmlmaxsoaparraysize	<Integer>	Read-write	XML Max Total SOAP Array Size. Protects against SOAP Array Abuse attack. Minimum value = 0 Maximum value = 1000000000
xmlmaxattributes	<Integer>	Read-write	Specify maximum number of attributes per XML element. Protects against overflow attacks.
xmlblockpi	<String>	Read-write	State if XML Block PI is ON or OFF.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Protects resources from denial of service attacks as SOAP messages cannot have processing instructions (PI) in messages. Possible values = ON, OFF
xmlmaxelementnamelength	<Integer>	Read-write	Specify the longest name of any element (including the expanded namespace) to protect against overflow attacks.
xmlmaxchardatalengthcheck	<String>	Read-write	State if XML Max CDATA length check is ON or OFF. Possible values = ON, OFF
xmlmaxnodescheck	<String>	Read-write	State if XML Max nodes check is ON or OFF. Possible values = ON, OFF
xmlblockexternalentities	<String>	Read-write	State if XML Block External Entities Check is ON or OFF. Protects against XML External Entity (XXE) attacks that force applications to parse untrusted external entities

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			(sources) in XML documents. Possible values = ON, OFF
xmlmaxattributescheck	<String>	Read-write	State if XML Max attributes check is ON or OFF. Possible values = ON, OFF
isautodeployed	<String>	Read-write	Is the rule auto deployed by dynamic profile ?. Possible values = AUTODEPLOYED, NOTAUTODEPLOYED
alertonly	<String>	Read-write	Send SNMP alert?. Possible values = ON, OFF
xmlmaxelementscheck	<String>	Read-write	State if XML Max elements check is ON or OFF. Possible values = ON, OFF
xmlmaxchardatalength	<Integer>	Read-write	Specify the maximum size of CDATA. Protects against overflow attacks and large quantities of unparsed data within XML messages. Minimum value = 0

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum value = 1000000000
comment	<String>	Read-write	Any comments about the purpose of profile, or other useful information about the profile.
xmlmaxnamespacescheck	<String>	Read-write	State if XML Max namespaces check is ON or OFF. Possible values = ON, OFF
xmldosurl	<String>	Read-write	XML DoS URL regular expression length.
xmlminfilesize	<Integer>	Read-write	Enforces minimum message size. Minimum value = 0 Maximum value = 1000000000
xmlblockdtd	<String>	Read-write	State if XML DTD is ON or OFF. Protects against recursive Document Type Declaration (DTD) entity expansion attacks. Also, SOAP messages cannot have DTDs in messages. . Possible values = ON, OFF

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
xmlmaxfilesizecheck	<String>	Read-write	State if XML Max file size check is ON or OFF. Possible values = ON, OFF
xmlmaxentityexpansionscheck	<String>	Read-write	State if XML Max Entity Expansions Check is ON or OFF. Possible values = ON, OFF
xmlmaxnamespaceurilength	<Integer>	Read-write	Specify the longest URI of any XML namespace. Protects against overflow attacks.
ruletype	<String>	Read-write	Specifies rule type of binding. Possible values = ALLOW, DENY
xmlmaxentityexpansions	<Integer>	Read-write	Specify maximum allowed number of entity expansions. Protects aganist Entity Expansion Attack.
xmlmaxnamespaceurilengthcheck	<String>	Read-write	State if XML Max namespace URI length check is ON or OFF. Possible values = ON, OFF
xmlmaxentityexpansiondepthcheck	<String>	Read-write	State if XML Max Entity Expansions

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Depth Check is ON or OFF. Possible values = ON, OFF
xmlmaxnamespaces	<Integer>	Read-write	Specify maximum number of active namespaces. Protects against overflow attacks.
xmlmaxelementdepthcheck	<String>	Read-write	State if XML Max element depth check is ON or OFF. Possible values = ON, OFF
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/appfwprofile_xmldosurl_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"appfwprofile_xmldosurl_binding":{

<b>"name":<String_value>,

</b>"comment":<String_value>,

"state":<String_value>,

"xmldosurl":<String_value>,

"xmlmaxelementdepthcheck":<String_value>,
```

```
"xmlmaxelementdepth":<Integer_value>,

"xmlmaxelementnamelengthcheck":<String_value>,

"xmlmaxelementnamelength":<Integer_value>,

"xmlmaxelementscheck":<String_value>,

"xmlmaxelements":<Integer_value>,

"xmlmaxelementchildrencheck":<String_value>,

"xmlmaxelementchildren":<Integer_value>,

"xmlmaxnodescheck":<String_value>,

"xmlmaxnodes":<Integer_value>,

"xmlmaxattributescheck":<String_value>,

"xmlmaxattributes":<Integer_value>,

"xmlmaxattributenamelengthcheck":<String_value>,

"xmlmaxattributenamelength":<Integer_value>,

"xmlmaxattributevaluelengthcheck":<String_value>,

"xmlmaxattributevaluelength":<Integer_value>,

"xmlmaxchardatalengthcheck":<String_value>,

"xmlmaxchardatalength":<Integer_value>,

"xmlmaxfilesizecheck":<String_value>,

"xmlmaxfilesize":<Integer_value>,

"xmlminfilesizecheck":<String_value>,

"xmlminfilesize":<Integer_value>,

"xmlblockpi":<String_value>,
```

```
"xmlblockdtd":<String_value>,

"xmlblockexternalentities":<String_value>,

"xmlmaxentityexpansionscheck":<String_value>,

"xmlmaxentityexpansions":<Integer_value>,

"xmlmaxentityexpansiondepthcheck":<String_value>,

"xmlmaxentityexpansiondepth":<Integer_value>,

"xmlmaxnamespacescheck":<String_value>,

"xmlmaxnamespaces":<Integer_value>,

"xmlmaxnamespaceurilengthcheck":<String_value>,

"xmlmaxnamespaceurilength":<Integer_value>,

"xmlsoaparraycheck":<String_value>,

"xmlmaxsoaparraysize":<Integer_value>,

"xmlmaxsoaparrayrank":<Integer_value>,

"isautodeployed":<String_value>,

"resourceid":<String_value>,

"ruletype":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_xmldosurl_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ appfwprofile_xmldosurl_binding/ name_value<String> ? **args=xmldosurl: <String_value> ,ruletype: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_xmldosurl_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ appfwprofile_xmldosurl_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of appfwprofile_xmldosurl_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_xmldosurl_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the appfwprofile_xmldosurl_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwprofile_xmldosurl_binding": [ {

"xmlmaxentityexpansiondepth":<Integer_value>,

"xmlmaxattributenamelengthcheck":<String_value>,

"xmlmaxattributenamelength":<Integer_value>,

"xmlmaxelementnamelengthcheck":<String_value>,

"xmlmaxelements":<Integer_value>,

"state":<String_value>,

"xmlmaxattributevaluelengthcheck":<String_value>,

"xmlmaxattributevaluelength":<Integer_value>,

"xmlminfilesizecheck":<String_value>,

"resourceid":<String_value>,

"xmlmaxfilesize":<Integer_value>,

"xmlmaxelementchildren":<Integer_value>,

"xmlmaxsoaparrayrank":<Integer_value>,

"name":<String_value>,

"xmlsoaparraycheck":<String_value>,

"xmlmaxelementchildrencheck":<String_value>,

"xmlmaxnodes":<Integer_value>,

"xmlmaxelementdepth":<Integer_value>,
```

```
"xmlmaxsoaparraysize":<Integer_value>,

"xmlmaxattributes":<Integer_value>,

"xmlblockpi":<String_value>,

"xmlmaxelementnamelength":<Integer_value>,

"xmlmaxchardatalengthcheck":<String_value>,

"xmlmaxnodescheck":<String_value>,

"xmlblockexternalentities":<String_value>,

"xmlmaxattributescheck":<String_value>,

"isautodeployed":<String_value>,

"alertonly":<String_value>,

"xmlmaxelementscheck":<String_value>,

"xmlmaxchardatalength":<Integer_value>,

"comment":<String_value>,

"xmlmaxnamespacescheck":<String_value>,

"xmldosurl":<String_value>,

"xmlminfilesize":<Integer_value>,

"xmlblockdtd":<String_value>,

"xmlmaxfilesizecheck":<String_value>,

"xmlmaxentityexpansionscheck":<String_value>,

"xmlmaxnamespaceurilength":<Integer_value>,

"ruletype":<String_value>,

"xmlmaxentityexpansions":<Integer_value>,
```

```
"xmlmaxnamespaceurilengthcheck":<String_value>,

"xmlmaxentityexpansiondepthcheck":<String_value>,

"xmlmaxnamespaces":<Integer_value>,

"xmlmaxelementdepthcheck":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_xmldosurl_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_xmldosurl_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwprofile_xmldosurl_binding": [ {

"xmlmaxentityexpansiondepth":<Integer_value>,
```

```
"xmlmaxattributenamelengthcheck":<String_value>,

"xmlmaxattributenamelength":<Integer_value>,

"xmlmaxelementnamelengthcheck":<String_value>,

"xmlmaxelements":<Integer_value>,

"state":<String_value>,

"xmlmaxattributevaluelengthcheck":<String_value>,

"xmlmaxattributevaluelength":<Integer_value>,

"xmlminfilesizecheck":<String_value>,

"resourceid":<String_value>,

"xmlmaxfilesize":<Integer_value>,

"xmlmaxelementchildren":<Integer_value>,

"xmlmaxsoaparrayrank":<Integer_value>,

"name":<String_value>,

"xmlsoaparraycheck":<String_value>,

"xmlmaxelementchildrencheck":<String_value>,

"xmlmaxnodes":<Integer_value>,

"xmlmaxelementdepth":<Integer_value>,

"xmlmaxsoaparraysize":<Integer_value>,

"xmlmaxattributes":<Integer_value>,

"xmlblockpi":<String_value>,

"xmlmaxelementnamelength":<Integer_value>,

"xmlmaxchardatalengthcheck":<String_value>,
```

```
"xmlmaxnodescheck":<String_value>,

"xmlblockexternalentities":<String_value>,

"xmlmaxattributescheck":<String_value>,

"isautodeployed":<String_value>,

"alertonly":<String_value>,

"xmlmaxelementscheck":<String_value>,

"xmlmaxchardatalength":<Integer_value>,

"comment":<String_value>,

"xmlmaxnamespacescheck":<String_value>,

"xmldosurl":<String_value>,

"xmlminfilesize":<Integer_value>,

"xmlblockdtd":<String_value>,

"xmlmaxfilesizecheck":<String_value>,

"xmlmaxentityexpansionscheck":<String_value>,

"xmlmaxnamespaceurilength":<Integer_value>,

"ruletype":<String_value>,

"xmlmaxentityexpansions":<Integer_value>,

"xmlmaxnamespaceurilengthcheck":<String_value>,

"xmlmaxentityexpansiondepthcheck":<String_value>,

"xmlmaxnamespaces":<Integer_value>,

"xmlmaxelementdepthcheck":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_xmldosurl_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"appfwprofile_xmldosurl_binding": [ { "__count": "#no"} ] }
```

appfwprofile_xmlsqlinjection_binding

Binding object showing the xmlsqlinjection that can be bound to appfwprofile.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
isautodeployed	<String>	Read-write	Is the rule auto deployed by dynamic profile ?. Possible values = AUTODEPLOYED, NOTAUTODEPLOYED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
alertonly	<String>	Read-write	Send SNMP alert?. Possible values = ON, OFF
isregex_xmlsql	<String>	Read-write	Is the XML SQL Injection exempted field name a regular expression?. Possible values = REGEX, NOTREGEX
xmlsqlinjection	<String>	Read-write	Exempt the specified URL from the XML SQL injection check. An XML SQL injection exemption (relaxation) consists of the following items: * Name. Name to exempt, as a string or a PCRE-format regular expression. * ISREGEX flag. REGEX if URL is a regular expression, NOTREGEX if URL is a fixed string. * Location. ELEMENT if the injection is located in an XML element, ATTRIBUTE if located in an XML attribute.
as_scan_location_xmlsql	<String>	Read-write	Location of SQL injection exception -

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			XML Element or Attribute. Possible values = ELEMENT, ATTRIBUTE
ruletype	<String>	Read-write	Specifies rule type of binding. Possible values = ALLOW, DENY
comment	<String>	Read-write	Any comments about the purpose of profile, or other useful information about the profile.
name	<String>	Read-write	Name of the profile to which to bind an exemption or rule. Minimum length = 1
state	<String>	Read-write	Enabled. Possible values = ENABLED, DISABLED
resourceid	<String>	Read-write	A "id" that identifies the rule.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET

- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/appfwprofile_xmlsqlinjection_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"appfwprofile_xmlsqlinjection_binding":{

<b>"name":<String_value>,

</b>"comment":<String_value>,

"state":<String_value>,

"xmlsqlinjection":<String_value>,

"isregex_xmlsql":<String_value>,

"as_scan_location_xmlsql":<String_value>,

"isautodeployed":<String_value>,

"resourceid":<String_value>,

"ruletype":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_xmlsqlinjection_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ appfwprofile_xmlsqlinjection_binding/ name_value<String> ? **args=xmlsqlinjection: <String_value> ,as_scan_location_xmlsql: <String_value> ,ruletype: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_xmlsqlinjection_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ appfwprofile_xmlsqlinjection_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of appfwprofile_xmlsqlinjection_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_xmlsqlinjection_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the appfwprofile_xmlsqlinjection_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwprofile_xmlsqlinjection_binding": [ {

"isautodeployed":<String_value>,

"alertonly":<String_value>,

"isregex_xmlsql":<String_value>,
```

```
"xmlsqlinjection":<String_value>,

"as_scan_location_xmlsql":<String_value>,

"ruletype":<String_value>,

"comment":<String_value>,

"name":<String_value>,

"state":<String_value>,

"resourceid":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_xmlsqlinjection_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_xmlsqlinjection_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwprofile_xmlsqlinjection_binding": [ {

"isautodeployed":<String_value>,

"alertonly":<String_value>,

"isregex_xmlsql":<String_value>,

"xmlsqlinjection":<String_value>,

"as_scan_location_xmlsql":<String_value>,

"ruletype":<String_value>,

"comment":<String_value>,

"name":<String_value>,

"state":<String_value>,

"resourceid":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_xmlsqlinjection_binding/name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"appfwprofile_xmlsqlinjection_binding": [ { "__count": "#no"} ] }
```

appfwprofile_xmlvalidationurl_binding

Binding object showing the xmlvalidationurl that can be bound to appfwprofile.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
xmlresponseschema	<String>	Read-write	XML Schema object for response validation.
xmlendpointcheck	<String>	Read-write	Modifies the behaviour of the Request URL validation w.r.t. the Service URL. If set to ABSOLUTE, the entire request URL is validated with the entire URL mentioned in Service of the associated WSDL. eg: Service URL: http://example.org/ExampleService, Request URL: http//example.com/ExampleService would FAIL the validation. If set to RELAIVE, only the non-hostname part of the request URL is

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			validated against the non-hostname part of the Service URL. eg: Service URL: http://example.org/ExampleService, Request URL: http//example.com/ExampleService would PASS the validation. Possible values = ABSOLUTE, RELATIVE
alertonly	<String>	Read-write	Send SNMP alert?. Possible values = ON, OFF
xmlrequestschema	<String>	Read-write	XML Schema object for request validation .
xmlwsdl	<String>	Read-write	WSDL object for soap request validation.
ruletype	<String>	Read-write	Specifies rule type of binding. Possible values = ALLOW, DENY
isautodeployed	<String>	Read-write	Is the rule auto deployed by dynamic profile ?. Possible values = AUTODEPLOYED, NOTAUTODEPLOYED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the profile to which to bind an exemption or rule. Minimum length = 1
xmlvalidatesoapenvelope	<String>	Read-write	Validate SOAP Evelope only. Possible values = ON, OFF
xmlvalidationurl	<String>	Read-write	XML Validation URL regular expression.
resourceid	<String>	Read-write	A "id" that identifies the rule.
comment	<String>	Read-write	Any comments about the purpose of profile, or other useful information about the profile.
state	<String>	Read-write	Enabled. Possible values = ENABLED, DISABLED
xmladditionalsoapheaders	<String>	Read-write	Allow addtional soap headers. Possible values = ON, OFF
xmlvalidateresponse	<String>	Read-write	Validate response message. Possible values = ON, OFF
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/appfwprofile_xmlvalidationurl_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"appfwprofile_xmlvalidationurl_binding":{

<b>"name":<String_value>,

</b>"comment":<String_value>,

"state":<String_value>,

"xmlvalidationurl":<String_value>,

"xmlrequestschema":<String_value>,

"xmlresponseschema":<String_value>,

"xmlwsdl":<String_value>,

"xmladditionalsoapheaders":<String_value>,

"xmlendpointcheck":<String_value>,

"xmlvalidatesoapenvelope":<String_value>,

"xmlvalidateresponse":<String_value>,

"isautodeployed":<String_value>,

"resourceid":<String_value>,

"ruletype":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_xmlvalidationurl_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ appfwprofile_xmlvalidationurl_binding/ name_value<String> ? **args=xmlvalidationurl: <String_value> ,ruletype: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_xmlvalidationurl_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ appfwprofile_xmlvalidationurl_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of appfwprofile_xmlvalidationurl_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_xmlvalidationurl_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the appfwprofile_xmlvalidationurl_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwprofile_xmlvalidationurl_binding": [ {

"xmlresponseschema":<String_value>,

"xmlendpointcheck":<String_value>,

"alertonly":<String_value>,

"xmlrequestschema":<String_value>,

"xmlwsdl":<String_value>,

"ruletype":<String_value>,

"isautodeployed":<String_value>,

"name":<String_value>,

"xmlvalidatesoapenvelope":<String_value>,

"xmlvalidationurl":<String_value>,

"resourceid":<String_value>,

"comment":<String_value>,

"state":<String_value>,

"xmladditionalsoapheaders":<String_value>,

"xmlvalidateresponse":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_xmlvalidationurl_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_xmlvalidationurl_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwprofile_xmlvalidationurl_binding": [ {

"xmlresponseschema":<String_value>,

"xmlendpointcheck":<String_value>,

"alertonly":<String_value>,

"xmlrequestschema":<String_value>,

"xmlwsdl":<String_value>,

"ruletype":<String_value>,
```

```
"isautodeployed":<String_value>,

"name":<String_value>,

"xmlvalidatesoapenvelope":<String_value>,

"xmlvalidationurl":<String_value>,

"resourceid":<String_value>,

"comment":<String_value>,

"state":<String_value>,

"xmladditionalsoapheaders":<String_value>,

"xmlvalidateresponse":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_xmlvalidationurl_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"appfwprofile_xmlvalidationurl_binding": [ { "__count": "#no"} ] }
```

appfwprofile_xmlwsiurl_binding

Binding object showing the xmlwsiurl that can be bound to appfwprofile.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
xmlwsiurl	<String>	Read-write	XML WS-I URL regular expression length.
alertonly	<String>	Read-write	Send SNMP alert?. Possible values = ON, OFF
resourceid	<String>	Read-write	A "id" that identifies the rule.
xmlwsichecks	<String>	Read-write	Specify a comma separated list of relevant WS-I rule IDs. (R1140, R1141).
ruletype	<String>	Read-write	Specifies rule type of binding. Possible values = ALLOW, DENY
name	<String>	Read-write	Name of the profile to which to bind an exemption or rule. Minimum length = 1
isautodeployed	<String>	Read-write	Is the rule auto deployed by dynamic profile ?.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = AUTODEPLOYED, NOTAUTODEPLOYED
state	<String>	Read-write	Enabled. Possible values = ENABLED, DISABLED
comment	<String>	Read-write	Any comments about the purpose of profile, or other useful information about the profile.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/appfwprofile_xmlwsiurl_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"appfwprofile_xmlwsiurl_binding":{

<b>"name":<String_value>,

</b>"comment":<String_value>,

"state":<String_value>,

"xmlwsiurl":<String_value>,

"xmlwsichecks":<String_value>,
```

```
"isautodeployed":<String_value>,

"resourceid":<String_value>,

"ruletype":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_xmlwsiurl_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ appfwprofile_xmlwsiurl_binding/ name_value<String> ? **args=xmlwsiurl: <String_value> ,ruletype: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_xmlwsiurl_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ appfwprofile_xmlwsiurl_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of appfwprofile_xmlwsiurl_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_xmlwsiurl_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the appfwprofile_xmlwsiurl_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwprofile_xmlwsiurl_binding": [ {

"xmlwsiurl":<String_value>,

"alertonly":<String_value>,

"resourceid":<String_value>,

"xmlwsichecks":<String_value>,

"ruletype":<String_value>,

"name":<String_value>,

"isautodeployed":<String_value>,

"state":<String_value>,

"comment":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_xmlwsiurl_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_xmlwsiurl_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwprofile_xmlwsiurl_binding": [ {

"xmlwsiurl":<String_value>,

"alertonly":<String_value>,

"resourceid":<String_value>,

"xmlwsichecks":<String_value>,

"ruletype":<String_value>,

"name":<String_value>,

"isautodeployed":<String_value>,
```

```
"state":<String_value>,

"comment":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_xmlwsiurl_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"appfwprofile_xmlwsiurl_binding": [ { "__count": "#no"} ] }
```

appfwprofile_xmlxss_binding

Binding object showing the xmlxss that can be bound to appfwprofile.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
comment	<String>	Read-write	Any comments about the purpose of

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			profile, or other useful information about the profile.
isregex_xmlxss	<String>	Read-write	Is the XML XSS exempted field name a regular expression?. Possible values = REGEX, NOTREGEX
ruletype	<String>	Read-write	Specifies rule type of binding. Possible values = ALLOW, DENY
alertonly	<String>	Read-write	Send SNMP alert?. Possible values = ON, OFF
isautodeployed	<String>	Read-write	Is the rule auto deployed by dynamic profile ?. Possible values = AUTODEPLOYED, NOTAUTODEPLOYED
as_scan_location_xmlxss	<String>	Read-write	Location of XSS injection exception - XML Element or Attribute. Possible values = ELEMENT, ATTRIBUTE
resourceid	<String>	Read-write	A "id" that identifies the rule.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
state	<String>	Read-write	Enabled. Possible values = ENABLED, DISABLED
xmlxss	<String>	Read-write	Exempt the specified URL from the XML cross-site scripting (XSS) check. An XML cross-site scripting exemption (relaxation) consists of the following items: * URL. URL to exempt, as a string or a PCRE-format regular expression. * ISREGEX flag. REGEX if URL is a regular expression, NOTREGEX if URL is a fixed string. * Location. ELEMENT if the attachment is located in an XML element, ATTRIBUTE if located in an XML attribute.
name	<String>	Read-write	Name of the profile to which to bind an exemption or rule. Minimum length = 1
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/appfwprofile_xmlxss_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"appfwprofile_xmlxss_binding":{

<b>"name":<String_value>,

</b>"comment":<String_value>,

"state":<String_value>,

"xmlxss":<String_value>,

"isregex_xmlxss":<String_value>,

"as_scan_location_xmlxss":<String_value>,

"isautodeployed":<String_value>,

"resourceid":<String_value>,

"ruletype":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_xmlxss_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ appfwprofile_xmlxss_binding/ name_value<String> ? **args=xmlxss: <String_value> ,as_scan_location_xmlxss: <String_value> ,ruletype: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_xmlxss_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ appfwprofile_xmlxss_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of appfwprofile_xmlxss_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_xmlxss_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the appfwprofile_xmlxss_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwprofile_xmlxss_binding": [ {

"comment":<String_value>,
```

```
"isregex_xmlxss":<String_value>,

"ruletype":<String_value>,

"alertonly":<String_value>,

"isautodeployed":<String_value>,

"as_scan_location_xmlxss":<String_value>,

"resourceid":<String_value>,

"state":<String_value>,

"xmlxss":<String_value>,

"name":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_xmlxss_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_xmlxss_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwprofile_xmlxss_binding": [ {

"comment":<String_value>,

"isregex_xmlxss":<String_value>,

"ruletype":<String_value>,

"alertonly":<String_value>,

"isautodeployed":<String_value>,

"as_scan_location_xmlxss":<String_value>,

"resourceid":<String_value>,

"state":<String_value>,

"xmlxss":<String_value>,

"name":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprofile_xmlxss_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"appfwprofile_xmlxss_binding": [ { "__count": "#no"} ] }
```

appfwprotofile

Configuration for gRPC protofile resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the gRPC schema object.
src	<String>	Read-write	Indicates source path of the gRPC schema file. Minimum length = 1 Maximum length = 2047
overwrite	<Boolean>	Read-write	Overwrite any existing gRPC schema object of the same name.
comment	<String>	Read-write	Comments associated with this gRPC schema file. Maximum length = 128

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
response	<String>	Read-only	gRPC import object response contents.
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- GET (ALL)
- GET
- IMPORT
- DELETE
- CHANGE

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

IMPORT

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprotofile? **action=Import HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"appfwprotofile":{

<b>"src":<String_value>,

</b><b>"name":<String_value>,

</b>"overwrite":<Boolean_value>,

"comment":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprotofile/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

CHANGE

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprotofile? **action=update HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"appfwprotofile":{

<b>"name":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprotofile **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "appfwprotofile": [ {

"name":<String_value>,

"response":<String_value>,

"src":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwprotofile/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/appfwprotofile/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/appfwprotofile/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of appfwprotofile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwprotofile": [ {

"name":<String_value>,

"response":<String_value>,

"src":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

appfwsettings

Configuration for AS settings resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
defaultprofile	<String>	Read-write	Profile to use when a connection does not match any policy. Default setting is APPFW_BYPASS, which sends unmatched connections back to the Citrix ADC without attempting to filter them further. Default value: APPFW_BYPASS

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum length = 1
undefaction	<String>	Read-write	Profile to use when an application firewall policy evaluates to undefined (UNDEF). An UNDEF event indicates an internal error condition. The APPFW_BLOCK built-in profile is the default setting. You can specify a different built-in or user-created profile as the UNDEF profile. Default value: APPFW_BLOCK Minimum length = 1
sessiontimeout	<Integer>	Read-write	Timeout, in seconds, after which a user session is terminated. Before continuing to use the protected web site, the user must establish a new session by opening a designated start URL. Default value: 900 Minimum value = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum value = 65535
learnratelimit	<Integer>	Read-write	Maximum number of connections per second that the application firewall learning engine examines to generate new relaxations for learning-enabled security checks. The application firewall drops any connections above this limit from the list of connections used by the learning engine. Default value: 400 Minimum value = 1 Maximum value = 1000
sessionlifetime	<Integer>	Read-write	Maximum amount of time (in seconds) that the application firewall allows a user session to remain active, regardless of user activity. After this time, the user session is terminated. Before continuing to use the protected web site, the user must establish a new

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			session by opening a designated start URL. A value of 0 represents infinite time. Default value: 0 Minimum value = 0 Maximum value = 2147483647
sessioncookiename	<String>	Read-write	Name of the session cookie that the application firewall uses to track user sessions. Must begin with a letter or number, and can consist of from 1 to 31 letters, numbers, and the hyphen (-) and underscore (_) symbols. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my cookie name"

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			or 'my cookie name'). Minimum length = 1
clientiploggingheader	<String>	Read-write	Name of an HTTP header that contains the IP address that the client used to connect to the protected web site or service.
importsizelimit	<Integer>	Read-write	Maximum cumulative size in bytes of all objects imported to Netscaler. The user is not allowed to import an object if the operation exceeds the currently configured limit. Default value: 134217728 Minimum value = 1 Maximum value = 268435456
signatureautoupdate	<String>	Read-write	Flag used to enable/disable auto update signatures. Default value: OFF Possible values = ON, OFF

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
signatureurl	<String>	Read-write	URL to download the mapping file from server. Default value: https://s3.amazonaws.com/NSAppFwSignatures/SignaturesMapping.xml
cookiepostencryptprefix	<String>	Read-write	String that is prepended to all encrypted cookie values. Minimum length = 1
logmalformedreq	<String>	Read-write	Log requests that are so malformed that application firewall parsing doesn't occur. Default value: ON Possible values = ON, OFF
geolocationlogging	<String>	Read-write	Enable Geo-Location Logging in CEF format logs. Default value: OFF Possible values = ON, OFF
ceflogging	<String>	Read-write	Enable CEF format logs.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: OFF Possible values = ON, OFF
entitydecoding	<String>	Read-write	Transform multibyte (double- or half-width) characters to single width characters. Default value: OFF Possible values = ON, OFF
useconfigurablesecretkey	<String>	Read-write	Use configurable secret key in AppFw operations. Default value: OFF Possible values = ON, OFF
sessionlimit	<Integer>	Read-write	Maximum number of sessions that the application firewall allows to be active, regardless of user activity. After the max_limit reaches, No more user session will be created . Default value: 100000 Minimum value = 0 Maximum value = 500000

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
malformedreqaction	<String[]>	Read-write	flag to define action on malformed requests that application firewall cannot parse. Possible values = none, block, log, stats
centralizedlearning	<String>	Read-write	Flag used to enable/ disable ADM centralized learning. Default value: OFF Possible values = ON, OFF
proxyserver	<String>	Read-write	Proxy Server IP to get updated signatures from AWS.
proxyport	<Integer>	Read-write	Proxy Server Port to get updated signatures from AWS. Default value: 8080 Range 1 - 65535 * in CLI is represented as 65535 in NITRO API
proxyusername	<String>	Read-write	Proxy Username. Minimum length = 1
proxypassword	<String>	Read-write	Password with which proxy user logs on.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum length = 1
cookieflags	<String>	Read-write	Add the specified flags to AppFW cookies. Available setttings function as follows: * None - Do not add flags to AppFW cookies. * HTTP Only - Add the HTTP Only flag to AppFW cookies, which prevent scripts from accessing them. * Secure - Add Secure flag to AppFW cookies. * All - Add both HTTPOnly and Secure flag to AppFW cookies. Default value: none Possible values = none, httpOnly, secure, all
learning	<String>	Read-only	Global learning option that overrides the profile level learning.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Available settings are as follows: * ON - Honor all profile level learn settings. * OFF - Avoids learning for all profiles ignoring profile level learn setting. Default value: ON Possible values = ON, OFF
builtin	<String[]>	Read-only	Flag to determine if application firewall settings is built-in or not. Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL
feature	<String>	Read-only	The feature to be checked while applying this config.
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- UPDATE
- UNSET

- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwsettings **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"appfwsettings":{

"defaultprofile":<String_value>,
```

```
"undefaction":<String_value>,

"sessiontimeout":<Integer_value>,

"learnratelimit":<Integer_value>,

"sessionlifetime":<Integer_value>,

"sessioncookiename":<String_value>,

"clientiploggingheader":<String_value>,

"importsizelimit":<Integer_value>,

"signatureautoupdate":<String_value>,

"signatureurl":<String_value>,

"cookiepostencryptprefix":<String_value>,

"logmalformedreq":<String_value>,

"geolocationlogging":<String_value>,

"ceflogging":<String_value>,

"entitydecoding":<String_value>,

"useconfigurablesecretkey":<String_value>,

"sessionlimit":<Integer_value>,

"malformedreqaction":<String[]_value>,

"centralizedlearning":<String_value>,

"proxyserver":<String_value>,

"proxyport":<Integer_value>,

"proxyusername":<String_value>,

"proxypassword":<String_value>,
```

```
"cookieflags":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwsettings? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"appfwsettings":{

"defaultprofile":true,

"undefaction":true,

"sessiontimeout":true,

"learnratelimit":true,

"sessionlifetime":true,

"sessioncookiename":true,

"clientiploggingheader":true,

"importsizelimit":true,

"signatureautoupdate":true,
```

```
"signatureurl":true,

"cookiepostencryptprefix":true,

"logmalformedreq":true,

"geolocationlogging":true,

"ceflogging":true,

"entitydecoding":true,

"useconfigurablesecretkey":true,

"sessionlimit":true,

"malformedreqaction":true,

"centralizedlearning":true,

"proxyserver":true,

"proxyport":true,

"proxyusername":true,

"proxypassword":true,

"cookieflags":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwsettings **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "appfwsettings": [ {

"defaultprofile":<String_value>,

"undefaction":<String_value>,

"sessiontimeout":<Integer_value>,

"learnratelimit":<Integer_value>,

"sessionlifetime":<Integer_value>,

"sessioncookiename":<String_value>,

"clientiploggingheader":<String_value>,

"importsizelimit":<Integer_value>,

"signatureautoupdate":<String_value>,

"signatureurl":<String_value>,

"cookiepostencryptprefix":<String_value>,

"logmalformedreq":<String_value>,

"geolocationlogging":<String_value>,

"ceflogging":<String_value>,
```

```
"entitydecoding":<String_value>,

"useconfigurablesecretkey":<String_value>,

"sessionlimit":<Integer_value>,

"malformedreqaction":<String[]_value>,

"learning":<String_value>,

"centralizedlearning":<String_value>,

"proxyserver":<String_value>,

"proxyport":<Integer_value>,

"proxyusername":<String_value>,

"proxypassword":<String_value>,

"cookieflags":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

appfwsignatures

Configuration for application firewall signatures XML configuration resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the signature object.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum length = 1
src	<String>	Read-write	URL (protocol, host, path, and file name) for the location from which to fetch the imported signatures object. NOTE: The import fails if the object to be imported is on an HTTPS server that requires client certificate authentication for access. Minimum length = 1 Maximum length = 2047
xslt	<String>	Read-write	XSLT file source. Maximum length = 2047
comment	<String>	Read-write	Any comments to preserve information about the signatures object. Maximum length = 128
overwrite	<Boolean>	Read-write	Overwrite any existing signatures object of the same name.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
merge	<Boolean>	Read-write	Merges the existing Signature with new signature rules.
preservedefactions	<Boolean>	Read-write	preserves def actions of signature rules.
sha1	<String>	Read-write	File path for sha1 file to validate signature file. Minimum length = 1 Maximum length = 2047
vendortype	<String>	Read-write	Third party vendor type for which WAF signatures has to be generated. Possible values = Snort
autoenablenewsignatures	<String>	Read-write	Flag used to enable/ disable auto enable new signatures. Default value: OFF Possible values = ON, OFF
ruleid	<Integer[]>	Read-write	Signature rule IDs to be Enabled/ Disabled. Minimum value = 1 Maximum value = 2000000

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
category	<String>	Read-write	Signature category to be Enabled/ Disabled. Minimum length = 1 Maximum length = 64
enabled	<String>	Read-write	Flag used to enable/ disable enable signature rule IDs/ Signature Category. Default value: ON Possible values = ON, OFF
action	<String[]>	Read-write	Signature action. Possible values = none, block, log, stats
mergedefault	<Boolean>	Read-write	Merges signature file with default signature file.
response	<String>	Read-only	.
encryptedversion	<Integer>	Read-only	Encrypted signature version.
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- DELETE
- GET (ALL)
- GET

- IMPORT
- CHANGE

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwsignatures/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

IMPORT

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwsignatures? **action=Import HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"appfwsignatures":{

<b>"src":<String_value>,

</b><b>"name":<String_value>,

</b>"xslt":<String_value>,

"comment":<String_value>,

"overwrite":<Boolean_value>,

"merge":<Boolean_value>,

"preservedefactions":<Boolean_value>,

"sha1":<String_value>,

"vendortype":<String_value>,

"autoenablenewsignatures":<String_value>,

"ruleid":<Integer[]_value>,

"category":<String_value>,

"enabled":<String_value>,

"action":<String[]_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

CHANGE

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwsignatures? **action=update HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"appfwsignatures":{

<b>"name":<String_value>,

</b>"mergedefault":<Boolean_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwsignatures **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "appfwsignatures": [ {

"name":<String_value>,

"response":<String_value>,

"src":<String_value>,

"encryptedversion":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwsignatures/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/appfwsignatures/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/appfwsignatures/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of appfwsignatures resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwsignatures": [ {

"name":<String_value>,

"response":<String_value>,

"src":<String_value>,

"encryptedversion":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

appfwtransactionrecords

Configuration for Application firewall transaction record resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
nodeid	<Integer>	Read-write	Unique number that identifies the cluster node.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum value = 0 Maximum value = 31
httptransactionid	<Integer>	Read-only	The http transaction identifier.
packetengineid	<Integer>	Read-only	The packet engine identifier.
appfwsessionid	<String>	Read-only	The session identifier set by the Application Firewall to track the user session.
profilename	<String>	Read-only	Application Firewall profile name.
url	<String>	Read-only	Request URL.
clientip	<String>	Read-only	The IP address of client.
destip	<String>	Read-only	The IP address of destination.
starttime	<String>	Read-only	Conveys time at which request processing started.
endtime	<String>	Read-only	Conveys time at which request processing end.
requestcontentlength	<Integer>	Read-only	The content length of request.
requestyields	<Integer>	Read-only	The number of times yielded during request processing

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			to send heart beat packets.
requestmaxprocessingtime	<Integer>	Read-only	The maximum processing time across yields during request processing.
responsecontentlength	<Integer>	Read-only	The content length of response.
responseyields	<Integer>	Read-only	The number of times yielded during response processing to send heart beat packets.
responsemaxprocessingtime	<Integer>	Read-only	The maximum processing time across yields during response processing.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwtransactionrecords **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/appfwtransactionrecords? **args=nodeid: <Integer_value>**

Use this query-parameter to get appfwtransactionrecords resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/config/appfwtransactionrecords? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/appfwtransactionrecords? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of appfwtransactionrecords resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/appfwtransactionrecords? **view=summary**

Use this query-parameter to get the summary output of appfwtransactionrecords resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/appfwtransactionrecords? **pagesize=#no;pageno=#no**

Use this query-parameter to get the appfwtransactionrecords resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "appfwtransactionrecords": [ {

nodeid:<Integer_value>"httptransactionid":<Integer_value>,

"packetengineid":<Integer_value>,

"appfwsessionid":<String_value>,

"profilename":<String_value>,

"url":<String_value>,

"clientip":<String_value>,

"destip":<String_value>,

"starttime":<String_value>,

"endtime":<String_value>,
```

```
"requestcontentlength":<Integer_value>,

"requestyields":<Integer_value>,

"requestmaxprocessingtime":<Integer_value>,

"responsecontentlength":<Integer_value>,

"responseyields":<Integer_value>,

"responsemaxprocessingtime":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwtransactionrecords? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "appfwtransactionrecords": [ { "__count": "#no"} ] }
```

appfwurlencodedformcontenttype

Configuration for Urlencoded form content type resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
urlencodedformcontenttypevalue	<String>	Read-write	Content type to be classified as urlencoded form. Minimum length = 1
isregex	<String>	Read-write	Is urlencoded form content type a regular expression?. Default value: NOTREGEX Possible values = REGEX, NOTREGEX
builtin	<String[]>	Read-only	Flag to determine if urlencoded form contenttype is built-in or not. Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL
feature	<String>	Read-only	The feature to be checked while applying this config.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwurlencodedformcontenttype **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"appfwurlencodedformcontenttype":{

<b>"urlencodedformcontenttypevalue":<String_value>,

</b>"isregex":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwurlencodedformcontenttype/ urlencodedformcontenttypevalue_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwurlencodedformcontenttype **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/ appfwurlencodedformcontenttype? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/appfwurlencodedformcontenttype? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of appfwurlencodedformcontenttype resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/appfwurlencodedformcontenttype? **view=summary**

Use this query-parameter to get the summary output of appfwurlencodedformcontenttype resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/appfwurlencodedformcontenttype? **pagesize=#no;pageno=#no**

Use this query-parameter to get the appfwurlencodedformcontenttype resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "appfwurlencodedformcontenttype": [ {

"urlencodedformcontenttypevalue":<String_value>,

"isregex":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,
```

```
"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwurlencodedformcontenttype/ urlencodedformcontenttypevalue_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/appfwurlencodedformcontenttype/ urlencodedformcontenttypevalue_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/appfwurlencodedformcontenttype/ urlencodedformcontenttypevalue_value<String> ? **view=summary**

Use this query-parameter to get the summary output of appfwurlencodedformcontenttype resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwurlencodedformcontenttype": [ {

"urlencodedformcontenttypevalue":<String_value>,
```

```
"isregex":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwurlencodedformcontenttype? **count=yes**
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "appfwurlencodedformcontenttype": [ { "__count": "#no"} ] }
```

appfwwsdl

Configuration for WSDL file resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the WSDL file to remove. Minimum length = 1
src	<String>	Read-write	URL (protocol, host, path, and name) of the WSDL file to be imported is stored. NOTE: The import fails if the object to be imported is on an HTTPS server that requires client certificate authentication for access. Minimum length = 1 Maximum length = 2047
comment	<String>	Read-write	Any comments to preserve information about the WSDL. Maximum length = 128
overwrite	<Boolean>	Read-write	Overwrite any existing WSDL of the same name.
response	<String>	Read-only	.
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- DELETE
- GET (ALL)
- GET
- IMPORT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwwsdl/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

IMPORT

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwwsdl? **action=Import HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"appfwwsdl":{

<b>"src":<String_value>,

</b><b>"name":<String_value>,

</b>"comment":<String_value>,

"overwrite":<Boolean_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwwsdl **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "appfwwsdl": [ {

"name":<String_value>,

"response":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwwsdl/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/appfwwsdl/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/appfwwsdl/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of appfwwsdl resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwwsdl": [ {

"name":<String_value>,

"response":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

appfwxmlcontenttype

Configuration for XML Content type resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
xmlcontenttypevalue	<String>	Read-write	Content type to be classified as XML. Minimum length = 1
isregex	<String>	Read-write	Is field name a regular expression?. Default value: NOTREGEX Possible values = REGEX, NOTREGEX

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
builtin	<String[]>	Read-only	Flag to determine if xmlcontenttype is built-in or not. Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL
feature	<String>	Read-only	The feature to be checked while applying this config.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwxmlcontenttype **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"appfwxmlcontenttype":{

<b>"xmlcontenttypevalue":<String_value>,

</b>"isregex":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwxmlcontenttype/ xmlcontenttypevalue_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwxmlcontenttype **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/appfwxmlcontenttype? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/appfwxmlcontenttype? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of appfwxmlcontenttype resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/appfwxmlcontenttype? **view=summary**

Use this query-parameter to get the summary output of appfwxmlcontenttype resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/appfwxmlcontenttype? **pagesize=#no;pageno=#no**

Use this query-parameter to get the appfwxmlcontenttype resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "appfwxmlcontenttype": [ {

"xmlcontenttypevalue":<String_value>,

"isregex":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwxmlcontenttype/ xmlcontenttypevalue_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/appfwxmlcontenttype/ xmlcontenttypevalue_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/appfwxmlcontenttype/ xmlcontenttypevalue_value<String> ? **view=summary**

Use this query-parameter to get the summary output of appfwxmlcontenttype resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwxmlcontenttype": [ {

"xmlcontenttypevalue":<String_value>,

"isregex":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwxmlcontenttype? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "appfwxmlcontenttype": [ { "__count": "#no"} ] }
```

appfwxmlerrorpage

Configuration for xml error page resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Indicates name of the imported xml error page to be removed. Minimum length = 1
src	<String>	Read-write	URL (protocol, host, path, and name) for the location from which to fetch the imported XML error object. NOTE: The import fails if the object to be imported is on an HTTPS server that requires client certificate

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			authentication for access. Minimum length = 1 Maximum length = 2047
comment	<String>	Read-write	Any comments to preserve information about the XML error object. Maximum length = 128
overwrite	<Boolean>	Read-write	Overwrite any existing XML error object of the same name.
response	<String>	Read-only	.
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- DELETE
- GET (ALL)
- GET
- IMPORT
- CHANGE

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwxmlerrorpage/ name_value<String>
HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

IMPORT

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwxmlerrorpage? **action=Import HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"appfwxmlerrorpage":{

<b>"src":<String_value>,

</b><b>"name":<String_value>,

</b>"comment":<String_value>,

"overwrite":<Boolean_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

CHANGE

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwxmlerrorpage? **action=update HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"appfwxmlerrorpage":{

<b>"name":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwxmlerrorpage **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "appfwxmlerrorpage": [ {

"name":<String_value>,

"response":<String_value>,

"src":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwxmlerrorpage/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/appfwxmlerrorpage/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/appfwxmlerrorpage/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of appfwxmlerrorpage resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwxmlerrorpage": [ {

"name":<String_value>,

"response":<String_value>,

"src":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

appfwxmlschema

Configuration for XML schema resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the XML Schema object to remove. Minimum length = 1
src	<String>	Read-write	URL (protocol, host, path, and file name) for the location from which to fetch the imported XML Schema. NOTE: The import fails if the object to be imported is on an HTTPS server that requires client certificate authentication for access. Minimum length = 1 Maximum length = 2047
comment	<String>	Read-write	Any comments to preserve information about the XML Schema object. Maximum length = 128
overwrite	<Boolean>	Read-write	Overwrite any existing XML Schema object of the same name.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
response	<String>	Read-only	.
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- DELETE
- GET (ALL)
- GET
- IMPORT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwxmlschema/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

IMPORT

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwxmlschema? **action=Import HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"appfwxmlschema":{

<b>"src":<String_value>,

</b><b>"name":<String_value>,

</b>"comment":<String_value>,

"overwrite":<Boolean_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwxmlschema **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "appfwxmlschema": [ {

"name":<String_value>,

"response":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/appfwxmlschema/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/appfwxmlschema/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/appfwxmlschema/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of appfwxmlschema resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwxmlschema": [ {

"name":<String_value>,

"response":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

appqoe

Appqoe

Application Level Quality of Experience configuration

NAME	DESCRIPTION
appqoeaction	Configuration for AppQoS action

NAME	DESCRIPTION
appqoecustomresp	Configuration for AppQoE custom response page
appqoeparameter	Configuration for QOS parameter
appqoepolicy	Configuration for AppQoS policy
appqoepolicy_binding	Binding object showing the resources that can be bound to appqoepolicy
appqoepolicy_lbvserver_binding	Binding object showing the lbvserver that can be bound to appqoepolicy

appqoeaction

Configuration for AppQoS action resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the AppQoE action. Must begin with a letter, number, or the underscore symbol (_). Other characters allowed, after the first character, are the hyphen (-), period (.) hash (#), space ( ), at (@), equals (=), and colon (:) characters. This is

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			a mandatory argument.
priority	<String>	Read-write	Priority for queuing the request. If server resources are not available for a request that matches the configured rule, this option specifies a priority for queuing the request until the server resources are available again. If priority is not configured then Lowest priority will be used to queue the request. Possible values = HIGH, MEDIUM, LOW, LOWEST
respondwith	<String>	Read-write	Responder action to be taken when the threshold is reached. Available settings function as follows: ACS - Serve content from an alternative content service Threshold : maxConn or delay NS - Serve from the Citrix ADC (built-in response)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Threshold : maxConn or delay. Possible values = ACS, NS
customfile	<String>	Read-write	name of the HTML page object to use as the response. Minimum length = 1
altcontentsvcname	<String>	Read-write	Name of the alternative content service to be used in the ACS. Minimum length = 1 Maximum length = 127
altcontentpath	<String>	Read-write	Path to the alternative content service to be used in the ACS. Minimum length = 4 Maximum length = 127
polqdepth	<Integer>	Read-write	Policy queue depth threshold value. When the policy queue size (number of requests queued for the policy binding this action is attached to) increases to the specified polqDepth value, subsequent requests are

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			dropped to the lowest priority level. Minimum value = 0 Maximum value = 4294967294
priqdepth	<Integer>	Read-write	Queue depth threshold value per priorirty level. If the queue size (number of requests in the queue of that particular priorirty) on the virtual server to which this policy is bound, increases to the specified qDepth value, subsequent requests are dropped to the lowest priority level. Minimum value = 0 Maximum value = 4294967294
maxconn	<Integer>	Read-write	Maximum number of concurrent connections that can be open for requests that matches with rule. Minimum value = 1 Maximum value = 4294967294
delay	<Integer>	Read-write	Delay threshold, in microseconds, for requests that match

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			the policy's rule. If the delay statistics gathered for the matching request exceed the specified delay, configured action triggered for that request, if there is no action then requests are dropped to the lowest priority level. Minimum value = 1 Maximum value = 599999999
dostrigexpression	<String>	Read-write	Optional expression to add second level check to trigger DoS actions. Specifically used for Analytics based DoS response generation.
dosaction	<String>	Read-write	DoS Action to take when vserver will be considered under DoS attack and corresponding rule matches. Mandatory if AppQoE actions are to be used for DoS attack prevention. Possible values = SimpleResponse, HICResponse

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
tcpprofile	<String>	Read-write	Bind TCP Profile based on L2/L3/L7 parameters. Minimum length = 1 Maximum length = 127
retryonreset	<String>	Read-write	Retry on TCP Reset. Default value: NO Possible values = YES, NO
retryontimeout	<Integer>	Read-write	Retry on request Timeout(in millisec) upon sending request to backend servers. Minimum value = 30 Maximum value = 2000
numretries	<Integer>	Read-write	Retry count. Default value: 3 Minimum value = 0 Maximum value = 7
hits	<Integer>	Read-only	.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD

- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/appqoeaction **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"appqoeaction":{

<b>"name":<String_value>,

</b>"priority":<String_value>,

"respondwith":<String_value>,

"customfile":<String_value>,

"altcontentsvcname":<String_value>,

"altcontentpath":<String_value>,

"polqdepth":<Integer_value>,

"priqdepth":<Integer_value>,

"maxconn":<Integer_value>,

"delay":<Integer_value>,

"dostrigexpression":<String_value>,

"dosaction":<String_value>,

"tcpprofile":<String_value>,

"retryonreset":<String_value>,

"retryontimeout":<Integer_value>,

"numretries":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/appqoeaction/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/appqoeaction **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"appqoeaction":{

<b>"name":<String_value>,

</b>"priority":<String_value>,

"altcontentsvcname":<String_value>,

"altcontentpath":<String_value>,

"polqdepth":<Integer_value>,

"priqdepth":<Integer_value>,

"maxconn":<Integer_value>,

"delay":<Integer_value>,
```

```
"dostrigexpression":<String_value>,

"dosaction":<String_value>,

"tcpprofile":<String_value>,

"retryonreset":<String_value>,

"retryontimeout":<Integer_value>,

"numretries":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/appqoeaction? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"appqoeaction":{

<b>"name":<String_value>,

</b>"priority":true,

"altcontentsvcname":true,

"altcontentpath":true,
```

```
"polqdepth":true,

"priqdepth":true,

"maxconn":true,

"delay":true,

"dosaction":true,

"tcpprofile":true,

"retryonreset":true,

"retryontimeout":true,

"numretries":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/appqoeaction **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/appqoeaction? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/appqoeaction? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of appqoeaction resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/appqoeaction? **view=summary**

Use this query-parameter to get the summary output of appqoeaction resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/appqoeaction? **pagesize=#no;pageno=#no**

Use this query-parameter to get the appqoeaction resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "appqoeaction": [ {

"name":<String_value>,

"hits":<Integer_value>,

"priority":<String_value>,

"respondwith":<String_value>,

"polqdepth":<Integer_value>,

"priqdepth":<Integer_value>,

"altcontentsvcname":<String_value>,

"altcontentpath":<String_value>,

"maxconn":<Integer_value>,
```

```
"delay":<Integer_value>,

"customfile":<String_value>,

"dostrigexpression":<String_value>,

"dosaction":<String_value>,

"tcpprofile":<String_value>,

"retryonreset":<String_value>,

"retryontimeout":<Integer_value>,

"numretries":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/appqoeaction/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/appqoeaction/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/appqoeaction/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of appqoeaction resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appqoeaction": [ {

"name":<String_value>,

"hits":<Integer_value>,

"priority":<String_value>,

"respondwith":<String_value>,

"polqdepth":<Integer_value>,

"priqdepth":<Integer_value>,

"altcontentsvcname":<String_value>,

"altcontentpath":<String_value>,

"maxconn":<Integer_value>,

"delay":<Integer_value>,

"customfile":<String_value>,

"dostrigexpression":<String_value>,

"dosaction":<String_value>,

"tcpprofile":<String_value>,

"retryonreset":<String_value>,

"retryontimeout":<Integer_value>,
```

```
"numretries":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/appqoeaction? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "appqoeaction": [ { "__count": "#no"} ] }
```

appqoecustomresp

Configuration for AppQoE custom response page resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
src	<String>	Read-write	.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum length = 1 Maximum length = 2047
name	<String>	Read-write	Indicates name of the custom response HTML page to import/update. Minimum length = 1 Maximum length = 31
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- IMPORT
- DELETE
- GET (ALL)
- COUNT
- CHANGE

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

IMPORT

URL: http:// <netscaler-ip-address> /nitro/v1/config/appqoecustomresp? **action=Import HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"appqoecustomresp":{

"src":<String_value>,

<b>"name":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/appqoecustomresp/ name_value<String>
HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

CHANGE

URL: http:// <netscaler-ip-address> /nitro/v1/config/appqoecustomresp? **action=update HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"appqoecustomresp":{

<b>"name":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/appqoecustomresp **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/appqoecustomresp? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/appqoecustomresp? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of appqoecustomresp resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/appqoecustomresp? **view=summary**

Use this query-parameter to get the summary output of appqoecustomresp resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/appqoecustomresp? **pagesize=#no;pageno=#no**

Use this query-parameter to get the appqoecustomresp resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "appqoecustomresp": [ {

"name":<String_value>,

"src":<String_value>,

"_nextgenapiresource":<String_value>
```

```
}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/appqoecustomresp? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "appqoecustomresp": [ { "__count": "#no"} ] }
```

appqoeparameter

Configuration for QOS parameter resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
sessionlife	<Integer>	Read-write	Time, in seconds, between the first time and the next time the AppQoE alternative content window is displayed.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			The alternative content window is displayed only once during a session for the same browser accessing a configured URL, so this parameter determines the length of a session. Default value: 300 Minimum value = 1 Maximum value = 4294967294
avgwaitingclient	<Integer>	Read-write	average number of client connections, that can sit in service waiting queue. Default value: 1000000 Minimum value = 0 Maximum value = 4294967294
maxaltrespbandwidth	<Integer>	Read-write	maximum bandwidth which will determine whether to send alternate content response. Default value: 100 Minimum value = 1 Maximum value = 4294967294

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
dosattackthresh	<Integer>	Read-write	average number of client connection that can queue up on vserver level without triggering DoS mitigation module. Default value: 2000 Minimum value = 0 Maximum value = 4294967294
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- UPDATE
- UNSET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/appqoeparameter **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"appqoeparameter":{

"sessionlife":<Integer_value>,

"avgwaitingclient":<Integer_value>,

"maxaltrespbandwidth":<Integer_value>,

"dosattackthresh":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/appqoeparameter? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"appqoeparameter":{

"sessionlife":true,

"avgwaitingclient":true,

"maxaltrespbandwidth":true,

"dosattackthresh":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/appqoeparameter **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "appqoeparameter": [ {

"sessionlife":<Integer_value>,

"avgwaitingclient":<Integer_value>,

"maxaltrespbandwidth":<Integer_value>,

"dosattackthresh":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

appqoepolicy

Configuration for AppQoS policy resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	. Minimum length = 1
rule	<String>	Read-write	Expression or name of a named expression, against which the request is evaluated. The policy is applied if the rule evaluates to true.
action	<String>	Read-write	Configured AppQoE action to trigger. Minimum length = 1
hits	<Integer>	Read-only	Number of hits.
_nextgenapiresource	<String>	Read-only	.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/appqoepolicy **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"appqoepolicy":{

<b>"name":<String_value>,

</b><b>"rule":<String_value>,

</b><b>"action":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/appqoepolicy/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/appqoepolicy **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"appqoepolicy":{

<b>"name":<String_value>,

</b>"rule":<String_value>,

"action":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/appqoepolicy **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/appqoepolicy? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/appqoepolicy? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of appqoepolicy resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/appqoepolicy? **view=summary**

Use this query-parameter to get the summary output of appqoepolicy resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/appqoepolicy? **pagesize=#no;pageno=#no**

Use this query-parameter to get the appqoepolicy resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "appqoepolicy": [ {

"name":<String_value>,

"rule":<String_value>,

"action":<String_value>,

"hits":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/appqoepolicy/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/appqoepolicy/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/appqoepolicy/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of appqoepolicy resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appqoepolicy": [ {

"name":<String_value>,

"rule":<String_value>,

"action":<String_value>,

"hits":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/appqoepolicy? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "appqoepolicy": [ { "__count": "#no"} ] }
```

appqoepolicy_binding

Binding object which returns the resources bound to appqoepolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	. Minimum length = 1
appqoepolicy_lbvserver_binding	<appqoepolicy_lbvserver_binding[]>	Read-only	lbvserver that can be bound to appqoepolicy.

Operations

(click to see Properties)

- GET

- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/appqoepolicy_binding/ name_value<String>
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "appqoepolicy_binding": [ {

"name":<String_value>,

"appqoepolicy_lbvserver_binding":<appqoepolicy_lbvserver_binding[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/appqoepolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/appqoepolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "appqoepolicy_binding": [ {

"name":<String_value>,

"appqoepolicy_lbvserver_binding":<appqoepolicy_lbvserver_binding[]_value>

}]}
```

appqoepolicy_lbvserver_binding

Binding object showing the lbvserver that can be bound to appqoepolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
boundto	<String>	Read-write	The name of the entity to which the policy is bound.
name	<String>	Read-write	. Minimum length = 1
gotopriorityexpression	<String>	Read-only	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
activepolicy	<Integer>	Read-only	.
bindpriority	<Integer>	Read-only	Specifies the binding of the policy. use only in display.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/appqoepolicy_lbvserver_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ appqoepolicy_lbvserver_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of appqoepolicy_lbvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/appqoepolicy_lbvserver_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the appqoepolicy_lbvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appqoepolicy_lbvserver_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"gotopriorityexpression":<String_value>,

"activepolicy":<Integer_value>,

"bindpriority":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/appqoepolicy_lbvserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/appqoepolicy_lbvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appqoepolicy_lbvserver_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"gotopriorityexpression":<String_value>,

"activepolicy":<Integer_value>,

"bindpriority":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/appqoepolicy_lbvserver_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"appqoepolicy_lbvserver_binding": [ { "__count": "#no"} ] }
```

audit

Audit

Audit configuration.

NAME	DESCRIPTION
auditmessageaction	Configuration for message action
auditmessages	Configuration for audit message
auditnslogaction	Configuration for ns log action
auditnslogglobal_auditnslogpolicy_binding	Binding object showing the auditnslogpolicy that can be bound to auditnslogglobal

NAME	DESCRIPTION
auditnslogglobal_binding	Binding object showing the resources that can be bound to auditnslogglobal
auditnslogparams	Configuration for ns log parameters
auditnslogpolicy	Configuration for ns log policy
auditnslogpolicy_aaagroup_binding	Binding object showing the aaagroup that can be bound to auditnslogpolicy
auditnslogpolicy_aaauser_binding	Binding object showing the aaauser that can be bound to auditnslogpolicy
auditnslogpolicy_appfwglobal_binding	Binding object showing the appfwglobal that can be bound to auditnslogpolicy
auditnslogpolicy_auditnslogglobal_binding	Binding object showing the auditnslogglobal that can be bound to auditnslogpolicy
auditnslogpolicy_authenticationvserver_binding	Binding object showing the authenticationvserver that can be bound to auditnslogpolicy
auditnslogpolicy_binding	Binding object showing the resources that can be bound to auditnslogpolicy
auditnslogpolicy_csvserver_binding	Binding object showing the csvserver that can be bound to auditnslogpolicy

NAME	DESCRIPTION
auditnslogpolicy_lbvserver_binding	Binding object showing the lbvserver that can be bound to auditnslogpolicy
auditnslogpolicy_systemglobal_binding	Binding object showing the systemglobal that can be bound to auditnslogpolicy
auditnslogpolicy_tmglobal_binding	Binding object showing the tmglobal that can be bound to auditnslogpolicy
auditnslogpolicy_vpnglobal_binding	Binding object showing the vpnglobal that can be bound to auditnslogpolicy
auditnslogpolicy_vpnvserver_binding	Binding object showing the vpnvserver that can be bound to auditnslogpolicy
auditsyslogaction	Configuration for system log action
auditsyslogglobal_auditsyslogpolicy_binding	Binding object showing the auditsyslogpolicy that can be bound to auditsyslogglobal
auditsyslogglobal_binding	Binding object showing the resources that can be bound to auditsyslogglobal
auditsyslogparams	Configuration for system log parameters
auditsyslogpolicy	Configuration for system log policy
auditsyslogpolicy_aaagroup_binding	Binding object showing the aaagroup that can be bound to auditsyslogpolicy

NAME	DESCRIPTION
auditsyslogpolicy_aaauser_binding	Binding object showing the aaauser that can be bound to auditsyslogpolicy
auditsyslogpolicy_auditsyslogglobal_binding	Binding object showing the auditsyslogglobal that can be bound to auditsyslogpolicy
auditsyslogpolicy_authenticationvserver_binding	Binding object showing the authenticationvserver that can be bound to auditsyslogpolicy
auditsyslogpolicy_binding	Binding object showing the resources that can be bound to auditsyslogpolicy
auditsyslogpolicy_csvserver_binding	Binding object showing the csvserver that can be bound to auditsyslogpolicy
auditsyslogpolicy_lbvserver_binding	Binding object showing the lbvserver that can be bound to auditsyslogpolicy
auditsyslogpolicy_rnatglobal_binding	Binding object showing the rnatglobal that can be bound to auditsyslogpolicy
auditsyslogpolicy_systemglobal_binding	Binding object showing the systemglobal that can be bound to auditsyslogpolicy
auditsyslogpolicy_tmglobal_binding	Binding object showing the tmglobal that can be bound to auditsyslogpolicy
auditsyslogpolicy_vpnglobal_binding	Binding object showing the vpnglobal that can be bound to auditsyslogpolicy

NAME	DESCRIPTION
auditsyslogpolicy_vpnvserver_binding	Binding object showing the vpnvserver that can be bound to auditsyslogpolicy

auditmessageaction

Configuration for message action resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the audit message action. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after the message action is added. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			marks (for example, "my message action" or 'my message action'). Minimum length = 1
loglevel	<String>	Read-write	Audit log level, which specifies the severity level of the log message being generated.. The following loglevels are valid: * EMERGENCY - Events that indicate an immediate crisis on the server. * ALERT - Events that might require action. * CRITICAL - Events that indicate an imminent server crisis. * ERROR - Events that indicate some type of error. * WARNING - Events that require action in the near future.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			* NOTICE - Events that the administrator should know about. * INFORMATIONAL - All but low-level events. * DEBUG - All events, in extreme detail. Possible values = EMERGENCY, ALERT, CRITICAL, ERROR, WARNING, NOTICE, INFORMATIONAL, DEBUG
stringbuilderexpr	<String>	Read-write	Default-syntax expression that defines the format and content of the log message.
logtonewnslog	<String>	Read-write	Send the message to the new nslog. Possible values = YES, NO
bypasssafetycheck	<String>	Read-write	Bypass the safety check and allow unsafe expressions. Default value: NO

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = YES, NO
loglevel1	<String>	Read-only	. Possible values = ALL, EMERGENCY, ALERT, CRITICAL, ERROR, WARNING, NOTICE, INFORMATIONAL, DEBUG, NONE
hits	<Integer>	Read-only	The number of times the action has been taken.
undefhits	<Integer>	Read-only	The number of times the action resulted in UNDEF.
referencecount	<Integer>	Read-only	The number of references to the action.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)

- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditmessageaction **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"auditmessageaction":{

<b>"name":<String_value>,

</b><b>"loglevel":<String_value>,

</b><b>"stringbuilderexpr":<String_value>,

</b>"logtonewnslog":<String_value>,

"bypasssafetycheck":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditmessageaction/ name_value<String>
HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditmessageaction **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"auditmessageaction":{

<b>"name":<String_value>,

</b>"loglevel":<String_value>,

"stringbuilderexpr":<String_value>,

"logtonewnslog":<String_value>,

"bypasssafetycheck":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditmessageaction? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"auditmessageaction":{

<b>"name":<String_value>,

</b>"logtonewnslog":true,

"bypasssafetycheck":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditmessageaction **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/auditmessageaction? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/auditmessageaction? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of auditmessageaction resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/auditmessageaction? **view=summary**

Use this query-parameter to get the summary output of auditmessageaction resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/auditmessageaction? **pagesize=#no;pageno=#no**

Use this query-parameter to get the auditmessageaction resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "auditmessageaction": [ {

"name":<String_value>,

"loglevel":<String_value>,

"loglevel1":<String_value>,

"stringbuilderexpr":<String_value>,

"logtonewnslog":<String_value>,

"bypasssafetycheck":<String_value>,

"hits":<Integer_value>,

"undefhits":<Integer_value>,

"referencecount":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditmessageaction/ name_value<String>
Query-parameters: attrs http:// <netscaler-ip-address> /nitro/v1/config/auditmessageaction/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/auditmessageaction/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of auditmessageaction resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "auditmessageaction": [ {

"name":<String_value>,

"loglevel":<String_value>,

"loglevel1":<String_value>,

"stringbuilderexpr":<String_value>,

"logtonewnslog":<String_value>,

"bypasssafetycheck":<String_value>,

"hits":<Integer_value>,

"undefhits":<Integer_value>,

"referencecount":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

```
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditmessageaction? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "auditmessageaction": [ { "__count": "#no"} ] }
```

auditmessages

Configuration for audit message resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
loglevel	<String[]>	Read-write	Audit log level filter, which specifies the types of events to display. The following loglevels are valid:

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			* ALL - All events. * EMERGENCY - Events that indicate an immediate crisis on the server. * ALERT - Events that might require action. * CRITICAL - Events that indicate an imminent server crisis. * ERROR - Events that indicate some type of error. * WARNING - Events that require action in the near future. * NOTICE - Events that the administrator should know about. * INFORMATIONAL - All but low-level events. * DEBUG - All events, in extreme detail.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ALL, EMERGENCY, ALERT, CRITICAL, ERROR, WARNING, NOTICE, INFORMATIONAL, DEBUG
numofmesgs	<Integer>	Read-write	Number of log messages to be displayed. Default value: 20 Minimum value = 1 Maximum value = 256
value	<String>	Read-only	The Audit message.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditmessages **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/auditmessages? **args=loglevel: <String _value> ,numofmesgs: <Integer_value>**

Use this query-parameter to get auditmessages resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/config/auditmessages? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/auditmessages? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of auditmessages resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/auditmessages? **view=summary**

Use this query-parameter to get the summary output of auditmessages resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/auditmessages? **pagesize=#no;pageno=#no**

Use this query-parameter to get the auditmessages resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "auditmessages": [ {

loglevel:<String[]_value>,numofmesgs:<Integer_value>"value":<String_value>
,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditmessages? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "auditmessages": [ { "__count": "#no"} ] }
```

auditnslogaction

Configuration for ns log action resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the nslog action. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after the nslog action is added. The following requirement applies

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my nslog action" or 'my nslog action'). Minimum length = 1
serverip	<String>	Read-write	IP address of the nslog server. Minimum length = 1
serverdomainname	<String>	Read-write	Auditserver name as a FQDN. Mutually exclusive with serverIP. Minimum length = 1 Maximum length = 255
domainresolveretry	<Integer>	Read-write	Time, in seconds, for which the Citrix ADC waits before sending another DNS query to resolve the host name of the audit server if the last query failed. Default value: 5 Minimum value = 5

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum value = 20939
serverport	<Integer>	Read-write	Port on which the nslog server accepts connections. Minimum value = 1
loglevel	<String[]>	Read-write	Audit log level, which specifies the types of events to log. Available settings function as follows: * ALL - All events. * EMERGENCY - Events that indicate an immediate crisis on the server. * ALERT - Events that might require action. * CRITICAL - Events that indicate an imminent server crisis. * ERROR - Events that indicate some type of error. * WARNING - Events that require action in the near future.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			* NOTICE - Events that the administrator should know about. * INFORMATIONAL - All but low-level events. * DEBUG - All events, in extreme detail. * NONE - No events. Possible values = ALL, EMERGENCY, ALERT, CRITICAL, ERROR, WARNING, NOTICE, INFORMATIONAL, DEBUG, NONE
dateformat	<String>	Read-write	Format of dates in the logs. Supported formats are: * MMDDYYYY - U.S. style month/date/year format. * DDMMYYYY - European style date/month/year format.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			* YYYYMMDD - ISO style year/ month/date format. Possible values = MMDDYYYY, DDMMYYYY, YYYYMMDD
logfacility	<String>	Read-write	Facility value, as defined in RFC 3164, assigned to the log message. Log facility values are numbers 0 to 7 (LOCAL0 through LOCAL7). Each number indicates where a specific message originated from, such as the Citrix ADC itself, the VPN, or external. Possible values = LOCAL0, LOCAL1, LOCAL2, LOCAL3, LOCAL4, LOCAL5, LOCAL6, LOCAL7
tcp	<String>	Read-write	Log TCP messages. Possible values = NONE, ALL
acl	<String>	Read-write	Log access control list (ACL) messages.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ENABLED, DISABLED
timezone	<String>	Read-write	Time zone used for date and timestamps in the logs. Available settings function as follows: * GMT_TIME. Coordinated Universal Time. * LOCAL_TIME. The server's timezone setting. Possible values = GMT_TIME, LOCAL_TIME
userdefinedauditlog	<String>	Read-write	Log user-configurable log messages to nslog. Setting this parameter to NO causes auditing to ignore all user-configured message actions. Setting this parameter to YES causes auditing to log user-configured message actions that meet the other logging criteria.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = YES, NO
appflowexport	<String>	Read-write	Export log messages to AppFlow collectors. Appflow collectors are entities to which log messages can be sent so that some action can be performed on them. Possible values = ENABLED, DISABLED
lsn	<String>	Read-write	Log the LSN messages. Possible values = ENABLED, DISABLED
alg	<String>	Read-write	Log the ALG messages. Possible values = ENABLED, DISABLED
subscriberlog	<String>	Read-write	Log subscriber session event information. Possible values = ENABLED, DISABLED
sslinterception	<String>	Read-write	Log SSL Interception event information.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ENABLED, DISABLED
urlfiltering	<String>	Read-write	Log URL filtering event information. Possible values = ENABLED, DISABLED
contentinspectionlog	<String>	Read-write	Log Content Inspection event information. Possible values = ENABLED, DISABLED
protocolviolations	<String>	Read-write	Log protocol violations. Possible values = ALL, NONE
denylistviolations	<String>	Read-write	Log denylist violations. Possible values = ENABLED, DISABLED
domainresolvenow	<Boolean>	Read-write	Immediately send a DNS query to resolve the server's domain name.
ip	<String>	Read-only	The resolved IP address of the auditserver.
builtin	<String[]>	Read-only	Indicates that a variable is a built-in

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			(SYSTEM INTERNAL) type. Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL
feature	<String>	Read-only	The feature to be checked while applying this config.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditnslogaction **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"auditnslogaction":{

<b>"name":<String_value>,

</b>"serverip":<String_value>,

"serverdomainname":<String_value>,

"domainresolveretry":<Integer_value>,

"serverport":<Integer_value>,

<b>"loglevel":<String[]_value>,

</b>"dateformat":<String_value>,
```

```
"logfacility":<String_value>,

"tcp":<String_value>,

"acl":<String_value>,

"timezone":<String_value>,

"userdefinedauditlog":<String_value>,

"appflowexport":<String_value>,

"lsn":<String_value>,

"alg":<String_value>,

"subscriberlog":<String_value>,

"sslinterception":<String_value>,

"urlfiltering":<String_value>,

"contentinspectionlog":<String_value>,

"protocolviolations":<String_value>,

"denylistviolations":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditnslogaction/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditnslogaction **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"auditnslogaction":{

<b>"name":<String_value>,

</b>"serverip":<String_value>,

"serverdomainname":<String_value>,

"domainresolveretry":<Integer_value>,

"domainresolvenow":<Boolean_value>,

"serverport":<Integer_value>,

"loglevel":<String[]_value>,

"dateformat":<String_value>,

"logfacility":<String_value>,

"tcp":<String_value>,

"acl":<String_value>,

"timezone":<String_value>,
```

```
"userdefinedauditlog":<String_value>,

"appflowexport":<String_value>,

"lsn":<String_value>,

"alg":<String_value>,

"subscriberlog":<String_value>,

"sslinterception":<String_value>,

"urlfiltering":<String_value>,

"contentinspectionlog":<String_value>,

"protocolviolations":<String_value>,

"denylistviolations":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditnslogaction? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"auditnslogaction":{

<b>"name":<String_value>,

</b>"serverport":true,

"loglevel":true,

"dateformat":true,

"logfacility":true,

"tcp":true,

"acl":true,

"timezone":true,

"userdefinedauditlog":true,

"appflowexport":true,

"lsn":true,

"alg":true,

"subscriberlog":true,

"sslinterception":true,

"contentinspectionlog":true,

"urlfiltering":true,

"protocolviolations":true,

"denylistviolations":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditnslogaction **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/auditnslogaction? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/auditnslogaction? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of auditnslogaction resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/auditnslogaction? **view=summary**

Use this query-parameter to get the summary output of auditnslogaction resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/auditnslogaction? **pagesize=#no;pageno=#no**

Use this query-parameter to get the auditnslogaction resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "auditnslogaction": [ {

"name":<String_value>,

"serverip":<String_value>,

"serverdomainname":<String_value>,

"domainresolveretry":<Integer_value>,

"domainresolvenow":<Boolean_value>,

"ip":<String_value>,

"serverport":<Integer_value>,

"loglevel":<String[]_value>,

"dateformat":<String_value>,

"logfacility":<String_value>,

"tcp":<String_value>,

"acl":<String_value>,

"timezone":<String_value>,

"userdefinedauditlog":<String_value>,

"appflowexport":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"lsn":<String_value>,

"alg":<String_value>,

"subscriberlog":<String_value>,
```

```
"sslinterception":<String_value>,

"urlfiltering":<String_value>,

"contentinspectionlog":<String_value>,

"protocolviolations":<String_value>,

"denylistviolations":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditnslogaction/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/auditnslogaction/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/auditnslogaction/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of auditnslogaction resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "auditnslogaction": [ {

"name":<String_value>,

"serverip":<String_value>,

"serverdomainname":<String_value>,

"domainresolveretry":<Integer_value>,

"domainresolvenow":<Boolean_value>,

"ip":<String_value>,

"serverport":<Integer_value>,

"loglevel":<String[]_value>,

"dateformat":<String_value>,

"logfacility":<String_value>,

"tcp":<String_value>,

"acl":<String_value>,

"timezone":<String_value>,

"userdefinedauditlog":<String_value>,

"appflowexport":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"lsn":<String_value>,
```

```
"alg":<String_value>,

"subscriberlog":<String_value>,

"sslinterception":<String_value>,

"urlfiltering":<String_value>,

"contentinspectionlog":<String_value>,

"protocolviolations":<String_value>,

"denylistviolations":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditnslogaction? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "auditnslogaction": [ { "__count": "#no"} ] }
```

auditnslogglobal_auditnslogpolicy_binding

Binding object showing the auditnslogpolicy that can be bound to auditnslogglobal.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
policyname	<String>	Read-write	Name of the audit nslog policy.
globalbindtype	<String>	Read-write	. Default value: SYSTEM_GLOBAL Possible values = SYSTEM_GLOBAL, VPN_GLOBAL, RNAT_GLOBAL, APPFW_GLOBAL, TM_GLOBAL
builtin	<String[]>	Read-write	Indicates that a variable is a built-in (SYSTEM INTERNAL) type. Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL
priority	<Integer>	Read-write	Specifies the priority of the policy. Minimum value = 1 Maximum value = 2147483647

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
numpol	<Integer>	Read-only	number of polices bound to label.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/auditnslogglobal_auditnslogpolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"auditnslogglobal_auditnslogpolicy_binding":{

<b>"policyname":<String_value>,

</b><b>"priority":<Integer_value>,

</b>"globalbindtype":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditnslogglobal_auditnslogpolicy_binding **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/auditnslogglobal_auditnslogpolicy_binding? **args=policyname: <String_value> ,globalbindtype: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditnslogglobal_auditnslogpolicy_binding **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/auditnslogglobal_auditnslogpolicy_binding? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of auditnslogglobal_auditnslogpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/auditnslogglobal_auditnslogpolicy_binding? **pagesize=#no;pageno=#no**

Use this query-parameter to get the auditnslogglobal_auditnslogpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "auditnslogglobal_auditnslogpolicy_binding": [ {

"policyname":<String_value>,

"globalbindtype":<String_value>,
```

```
"builtin":<String[]_value>,

"priority":<Integer_value>,

"numpol":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditnslogglobal_auditnslogpolicy_binding?**count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "auditnslogglobal_auditnslogpolicy_binding": [ { "__count": "#no"} ] }
```

auditnslogglobal_binding

Binding object which returns the resources bound to auditnslogglobal.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
auditnslogglobal_auditnslogpolicy_binding	<auditnslogglobal_auditnslogpolicy_binding[]>	Read-write	auditnslogpolicy that can be bound to auditnslogglobal.

Operations

(click to see Properties)

- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditnslogglobal_binding

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "auditnslogglobal_binding": [ {

"auditnslogglobal_auditnslogpolicy_binding":<auditnslogglobal_auditnslogpo
licy_binding[]_value>

}]}
```

auditnslogparams

Configuration for ns log parameters resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
serverip	<String>	Read-write	IP address of the nslog server. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
serverport	<Integer>	Read-write	Port on which the nslog server accepts connections. Minimum value = 1
dateformat	<String>	Read-write	Format of dates in the logs. Supported formats are: * MMDDYYYY - U.S. style month/date/year format. * DDMMYYYY - European style date/month/year format. * YYYYMMDD - ISO style year/month/date format. Possible values = MMDDYYYY, DDMMYYYY, YYYYMMDD
loglevel	<String[]>	Read-write	Types of information to be logged. Available settings function as follows: * ALL - All events. * EMERGENCY - Events that indicate

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			an immediate crisis on the server. * ALERT - Events that might require action. * CRITICAL - Events that indicate an imminent server crisis. * ERROR - Events that indicate some type of error. * WARNING - Events that require action in the near future. * NOTICE - Events that the administrator should know about. * INFORMATIONAL - All but low-level events. * DEBUG - All events, in extreme detail. * NONE - No events. Possible values = ALL, EMERGENCY, ALERT, CRITICAL,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			ERROR, WARNING, NOTICE, INFORMATIONAL, DEBUG, NONE
logfacility	<String>	Read-write	Facility value, as defined in RFC 3164, assigned to the log message. Log facility values are numbers 0 to 7 (LOCAL0 through LOCAL7). Each number indicates where a specific message originated from, such as the Citrix ADC itself, the VPN, or external. Possible values = LOCAL0, LOCAL1, LOCAL2, LOCAL3, LOCAL4, LOCAL5, LOCAL6, LOCAL7
tcp	<String>	Read-write	Configure auditing to log TCP messages. Possible values = NONE, ALL
acl	<String>	Read-write	Configure auditing to log access control list (ACL) messages. Possible values = ENABLED, DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
timezone	<String>	Read-write	Time zone used for date and timestamps in the logs. Supported settings are: * GMT_TIME - Coordinated Universal Time. * LOCAL_TIME - Use the server's timezone setting. Possible values = GMT_TIME, LOCAL_TIME
userdefinedauditlog	<String>	Read-write	Log user-configurable log messages to nslog. Setting this parameter to NO causes auditing to ignore all user-configured message actions. Setting this parameter to YES causes auditing to log user-configured message actions that meet the other logging criteria. Possible values = YES, NO

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
appflowexport	<String>	Read-write	Export log messages to AppFlow collectors. Appflow collectors are entities to which log messages can be sent so that some action can be performed on them. Possible values = ENABLED, DISABLED
lsn	<String>	Read-write	Log the LSN messages. Possible values = ENABLED, DISABLED
alg	<String>	Read-write	Log the ALG messages. Possible values = ENABLED, DISABLED
subscriberlog	<String>	Read-write	Log subscriber session event information. Possible values = ENABLED, DISABLED
sslinterception	<String>	Read-write	Log SSL Interception event information. Possible values = ENABLED, DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
urlfiltering	<String>	Read-write	Log URL filtering event information. Possible values = ENABLED, DISABLED
contentinspectionlog	<String>	Read-write	Log Content Inspection event information. Possible values = ENABLED, DISABLED
protocolviolations	<String>	Read-write	Log protocol violations. Possible values = ALL, NONE
denylistviolations	<String>	Read-write	Log denylist violations. Possible values = ENABLED, DISABLED
builtin	<String[]>	Read-only	Indicates that a variable is a built-in (SYSTEM INTERNAL) type. Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL
feature	<String>	Read-only	The feature to be checked while applying this config.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- UPDATE
- UNSET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditnslogparams **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"auditnslogparams":{

"serverip":<String_value>,

"serverport":<Integer_value>,

"dateformat":<String_value>,

"loglevel":<String[]_value>,

"logfacility":<String_value>,

"tcp":<String_value>,

"acl":<String_value>,

"timezone":<String_value>,

"userdefinedauditlog":<String_value>,

"appflowexport":<String_value>,

"lsn":<String_value>,

"alg":<String_value>,

"subscriberlog":<String_value>,

"sslinterception":<String_value>,

"urlfiltering":<String_value>,

"contentinspectionlog":<String_value>,

"protocolviolations":<String_value>,
```

```
"denylistviolations":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditnslogparams? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"auditnslogparams":{

"serverip":true,

"serverport":true,

"loglevel":true,

"dateformat":true,

"logfacility":true,

"tcp":true,

"acl":true,

"timezone":true,

"userdefinedauditlog":true,
```

```
"appflowexport":true,

"lsn":true,

"alg":true,

"subscriberlog":true,

"sslinterception":true,

"urlfiltering":true,

"contentinspectionlog":true,

"protocolviolations":true,

"denylistviolations":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditnslogparams **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "auditnslogparams": [ {

"name":<String_value>,

"serverip":<String_value>,

"serverport":<Integer_value>,

"dateformat":<String_value>,

"loglevel":<String[]_value>,

"logfacility":<String_value>,

"tcp":<String_value>,

"acl":<String_value>,

"timezone":<String_value>,

"userdefinedauditlog":<String_value>,

"appflowexport":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"lsn":<String_value>,

"alg":<String_value>,

"subscriberlog":<String_value>,

"sslinterception":<String_value>,

"urlfiltering":<String_value>,

"contentinspectionlog":<String_value>,

"protocolviolations":<String_value>,
```

```
"denylistviolations":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

auditnslogpolicy

Configuration for ns log policy resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the policy. Must begin with a letter, number, or the underscore character (_), and must consist only of letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore characters. Cannot be changed after the nslog policy is added. The following requirement applies only to the Citrix ADC CLI:

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my nslog policy" or 'my nslog policy'). Minimum length = 1
rule	<String>	Read-write	Name of the Citrix ADC named rule, or an expression, that defines the messages to be logged to the nslog server. Minimum length = 1
action	<String>	Read-write	Nslog server action that is performed when this policy matches. NOTE: An nslog server action must be associated with an nslog audit policy. Minimum length = 1
builtin	<String[]>	Read-only	Indicates that a variable is a built-in (SYSTEM INTERNAL) type. Possible values = MODIFIABLE, DELETABLE,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			IMMUTABLE, PARTITION_ALL
feature	<String>	Read-only	The feature to be checked while applying this config.
expressiontype	<String>	Read-only	Type of policy (Classic/Advanced). Possible values = Classic Policy, Advanced Policy
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditnslogpolicy **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"auditnslogpolicy":{

<b>"name":<String_value>,

</b><b>"rule":<String_value>,

</b><b>"action":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditnslogpolicy/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditnslogpolicy **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"auditnslogpolicy":{

<b>"name":<String_value>,

</b>"rule":<String_value>,

"action":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditnslogpolicy **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/auditnslogpolicy? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/auditnslogpolicy? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of auditnslogpolicy resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/auditnslogpolicy? **view=summary**

Use this query-parameter to get the summary output of auditnslogpolicy resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/auditnslogpolicy? **pagesize=#no;pageno=#no**

Use this query-parameter to get the auditnslogpolicy resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "auditnslogpolicy": [ {

"name":<String_value>,

"rule":<String_value>,

"action":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"expressiontype":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditnslogpolicy/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/auditnslogpolicy/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/auditnslogpolicy/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of auditnslogpolicy resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "auditnslogpolicy": [ {

"name":<String_value>,

"rule":<String_value>,

"action":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"expressiontype":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditnslogpolicy? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "auditnslogpolicy": [ { "__count": "#no"} ] }
```

auditnslogpolicy_aaagroup_binding

Binding object showing the aaagroup that can be bound to auditnslogpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the policy. Minimum length = 1
boundto	<String>	Read-write	The entity name to which policy is bound.
activepolicy	<Integer>	Read-only	.
priority	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditnslogpolicy_aaagroup_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ auditnslogpolicy_aaagroup_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of auditnslogpolicy_aaagroup_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/auditnslogpolicy_aaagroup_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the auditnslogpolicy_aaagroup_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "auditnslogpolicy_aaagroup_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"activepolicy":<Integer_value>,

"priority":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditnslogpolicy_aaagroup_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/auditnslogpolicy_aaagroup_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "auditnslogpolicy_aaagroup_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"activepolicy":<Integer_value>,

"priority":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditnslogpolicy_aaagroup_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"auditnslogpolicy_aaagroup_binding": [ { "__count": "#no"} ] }
```

auditnslogpolicy_aaauser_binding

Binding object showing the aaauser that can be bound to auditnslogpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the policy. Minimum length = 1
boundto	<String>	Read-write	The entity name to which policy is bound.
priority	<Integer>	Read-only	.
activepolicy	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditnslogpolicy_aaauser_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ auditnslogpolicy_aaauser_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of auditnslogpolicy_aaauser_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/auditnslogpolicy_aaauser_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the auditnslogpolicy_aaauser_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "auditnslogpolicy_aaauser_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"priority":<Integer_value>,

"activepolicy":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditnslogpolicy_aaauser_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/auditnslogpolicy_aaauser_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "auditnslogpolicy_aaauser_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"priority":<Integer_value>,

"activepolicy":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditnslogpolicy_aaauser_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"auditnslogpolicy_aaauser_binding": [ { "__count": "#no"} ] }
```

auditnslogpolicy_appfwglobal_binding

Binding object showing the appfwglobal that can be bound to auditnslogpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the policy. Minimum length = 1
boundto	<String>	Read-write	The entity name to which policy is bound.
activepolicy	<Integer>	Read-only	.
priority	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.
- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of

creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditnslogpolicy_appfwglobal_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ auditnslogpolicy_appfwglobal_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of auditnslogpolicy_appfwglobal_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/auditnslogpolicy_appfwglobal_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the auditnslogpolicy_appfwglobal_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "auditnslogpolicy_appfwglobal_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"activepolicy":<Integer_value>,

"priority":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditnslogpolicy_appfwglobal_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/auditnslogpolicy_appfwglobal_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "auditnslogpolicy_appfwglobal_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"activepolicy":<Integer_value>,

"priority":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditnslogpolicy_appfwglobal_binding/name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"auditnslogpolicy_appfwglobal_binding": [ { "__count": "#no"} ] }
```

auditnslogpolicy_auditnslogglobal_binding

Binding object showing the auditnslogglobal that can be bound to auditnslogpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the policy. Minimum length = 1
boundto	<String>	Read-write	The entity name to which policy is bound.
priority	<Integer>	Read-only	.
activepolicy	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditnslogpolicy_auditnslogglobal_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ auditnslogpolicy_auditnslogglobal_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of auditnslogpolicy_auditnslogglobal_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ auditnslogpolicy_auditnslogglobal_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the auditnslogpolicy_auditnslogglobal_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "auditnslogpolicy_auditnslogglobal_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"priority":<Integer_value>,

"activepolicy":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditnslogpolicy_auditnslogglobal_binding
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/auditnslogpolicy_auditnslogglobal_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "auditnslogpolicy_auditnslogglobal_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"priority":<Integer_value>,

"activepolicy":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditnslogpolicy_auditnslogglobal_binding/name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"auditnslogpolicy_auditnslogglobal_binding": [ { "__count": "#no"} ] }
```

auditnslogpolicy_authenticationvserver_binding

Binding object showing the authenticationvserver that can be bound to auditnslogpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the policy. Minimum length = 1
boundto	<String>	Read-write	The entity name to which policy is bound.
activepolicy	<Integer>	Read-only	.
priority	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/ auditnslogpolicy_authenticationvserver_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/auditnslogpolicy_authenticationvserver_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of auditnslogpolicy_authenticationvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ auditnslogpolicy_authenticationvserver_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the auditnslogpolicy_authenticationvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "auditnslogpolicy_authenticationvserver_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"activepolicy":<Integer_value>,

"priority":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditnslogpolicy_authenticationvserver_binding
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/auditnslogpolicy_authenticationvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "auditnslogpolicy_authenticationvserver_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"activepolicy":<Integer_value>,

"priority":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/ auditnslogpolicy_authenticationvserver_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"auditnslogpolicy_authenticationvserver_binding": [ { "__count":
"#no"} ] }
```

auditnslogpolicy_binding

Binding object which returns the resources bound to auditnslogpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the policy. Minimum length = 1
auditnslogpolicy_aaauser_binding	<auditnslogpolicy_aaauser_binding[]>	Read-only	aaauser that can be bound to auditnslogpolicy.
auditnslogpolicy_authenticationvserver_binding	<auditnslogpolicy_authenticationvserver_binding[]>	Read-only	authenticationvserver that can be bound to auditnslogpolicy.
auditnslogpolicy_lbvserver_binding	<auditnslogpolicy_lbvserver_binding[]>	Read-only	lbvserver that can be bound to auditnslogpolicy.
auditnslogpolicy_appfwglobal_binding	<auditnslogpolicy_appfwglobal_binding[]>	Read-only	appfwglobal that can be bound to auditnslogpolicy.
auditnslogpolicy_aaagroup_binding	<auditnslogpolicy_aaagroup_binding[]>	Read-only	aaagroup that can be bound to auditnslogpolicy.
auditnslogpolicy_vpnglobal_binding	<auditnslogpolicy_vpnglobal_binding[]>	Read-only	vpnglobal that can be bound to auditnslogpolicy.
auditnslogpolicy_vpnvserver_binding	<auditnslogpolicy_vpnvserver_binding[]>	Read-only	vpnvserver that can be bound to auditnslogpolicy.
auditnslogpolicy_csvserver_binding	<auditnslogpolicy_csvserver_binding[]>	Read-only	csvserver that can be bound to auditnslogpolicy.
auditnslogpolicy_systemglobal_binding	<auditnslogpolicy_systemglobal_binding[]>	Read-only	systemglobal that can be bound to auditnslogpolicy.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
auditnslogpolicy_auditnslogglobal_binding	<auditnslogpolicy_auditnslogglobal_binding[]>	Read-only	auditnslogglobal that can be bound to auditnslogpolicy.
auditnslogpolicy_tmglobal_binding	<auditnslogpolicy_tmglobal_binding[]>	Read-only	tmglobal that can be bound to auditnslogpolicy.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditnslogpolicy_binding/ name_value<String>
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "auditnslogpolicy_binding": [ {

"name":<String_value>,

"auditnslogpolicy_aaagroup_binding":<auditnslogpolicy_aaagroup_binding[]_v
alue>,

"auditnslogpolicy_auditnslogglobal_binding":<auditnslogpolicy_auditnsloggl
obal_binding[]_value>,

"auditnslogpolicy_lbvserver_binding":<auditnslogpolicy_lbvserver_binding[]
_value>,

"auditnslogpolicy_aaauser_binding":<auditnslogpolicy_aaauser_binding[]_val
ue>,

"auditnslogpolicy_authenticationvserver_binding":<auditnslogpolicy_authent
icationvserver_binding[]_value>,

"auditnslogpolicy_appfwglobal_binding":<auditnslogpolicy_appfwglobal_bindi
ng[]_value>,
```

```
"auditnslogpolicy_vpnvserver_binding":<auditnslogpolicy_vpnvserver_binding
[]_value>,

"auditnslogpolicy_systemglobal_binding":<auditnslogpolicy_systemglobal_bin
ding[]_value>,

"auditnslogpolicy_tmglobal_binding":<auditnslogpolicy_tmglobal_binding[]_v
alue>,

"auditnslogpolicy_vpnglobal_binding":<auditnslogpolicy_vpnglobal_binding[]
_value>,

"auditnslogpolicy_csvserver_binding":<auditnslogpolicy_csvserver_binding[]
_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditnslogpolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/auditnslogpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "auditnslogpolicy_binding": [ {

"name":<String_value>,

"auditnslogpolicy_aaagroup_binding":<auditnslogpolicy_aaagroup_binding[]_value>,

"auditnslogpolicy_auditnslogglobal_binding":<auditnslogpolicy_auditnslogglobal_binding[]_value>,

"auditnslogpolicy_lbvserver_binding":<auditnslogpolicy_lbvserver_binding[]_value>,

"auditnslogpolicy_aaauser_binding":<auditnslogpolicy_aaauser_binding[]_value>,

"auditnslogpolicy_authenticationvserver_binding":<auditnslogpolicy_authenticationvserver_binding[]_value>,

"auditnslogpolicy_appfwglobal_binding":<auditnslogpolicy_appfwglobal_binding[]_value>,

"auditnslogpolicy_vpnvserver_binding":<auditnslogpolicy_vpnvserver_binding[]_value>,

"auditnslogpolicy_systemglobal_binding":<auditnslogpolicy_systemglobal_binding[]_value>,

"auditnslogpolicy_tmglobal_binding":<auditnslogpolicy_tmglobal_binding[]_value>,

"auditnslogpolicy_vpnglobal_binding":<auditnslogpolicy_vpnglobal_binding[]_value>,

"auditnslogpolicy_csvserver_binding":<auditnslogpolicy_csvserver_binding[]_value>

}]}
```

auditnslogpolicy_csvserver_binding

Binding object showing the csvserver that can be bound to auditnslogpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the policy. Minimum length = 1
boundto	<String>	Read-write	The entity name to which policy is bound.
activepolicy	<Integer>	Read-only	.
priority	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.
- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of

creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditnslogpolicy_csvserver_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ auditnslogpolicy_csvserver_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of auditnslogpolicy_csvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/auditnslogpolicy_csvserver_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the auditnslogpolicy_csvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "auditnslogpolicy_csvserver_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"activepolicy":<Integer_value>,

"priority":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditnslogpolicy_csvserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/auditnslogpolicy_csvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "auditnslogpolicy_csvserver_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"activepolicy":<Integer_value>,

"priority":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditnslogpolicy_csvserver_binding/name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"auditnslogpolicy_csvserver_binding": [ { "__count": "#no"} ] }
```

auditnslogpolicy_lbvserver_binding

Binding object showing the lbvserver that can be bound to auditnslogpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the policy. Minimum length = 1
boundto	<String>	Read-write	The entity name to which policy is bound.
priority	<Integer>	Read-only	.
activepolicy	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditnslogpolicy_lbvserver_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ auditnslogpolicy_lbvserver_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of auditnslogpolicy_lbvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/auditnslogpolicy_lbvserver_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the auditnslogpolicy_lbvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "auditnslogpolicy_lbvserver_binding": [ {

"name":<String_value>,
```

```
"boundto":<String_value>,

"priority":<Integer_value>,

"activepolicy":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditnslogpolicy_lbvserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/auditnslogpolicy_lbvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "auditnslogpolicy_lbvserver_binding": [ {

"name":<String_value>,

"boundto":<String_value>,
```

```
"priority":<Integer_value>,

"activepolicy":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditnslogpolicy_lbvserver_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"auditnslogpolicy_lbvserver_binding": [ { "__count": "#no"} ] }
```

auditnslogpolicy_systemglobal_binding

Binding object showing the systemglobal that can be bound to auditnslogpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
boundto	<String>	Read-write	The entity name to which policy is bound.
name	<String>	Read-write	Name of the policy. Minimum length = 1
activepolicy	<Integer>	Read-only	.
priority	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditnslogpolicy_systemglobal_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ auditnslogpolicy_systemglobal_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of auditnslogpolicy_systemglobal_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/auditnslogpolicy_systemglobal_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the auditnslogpolicy_systemglobal_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "auditnslogpolicy_systemglobal_binding": [ {

"boundto":<String_value>,
```

```
"name":<String_value>,

"activepolicy":<Integer_value>,

"priority":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditnslogpolicy_systemglobal_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/auditnslogpolicy_systemglobal_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "auditnslogpolicy_systemglobal_binding": [ {

"boundto":<String_value>,

"name":<String_value>,
```

```
"activepolicy":<Integer_value>,

"priority":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditnslogpolicy_systemglobal_binding/name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"auditnslogpolicy_systemglobal_binding": [ { "__count": "#no"} ] }
```

auditnslogpolicy_tmglobal_binding

Binding object showing the tmglobal that can be bound to auditnslogpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the policy. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
boundto	<String>	Read-write	The entity name to which policy is bound.
priority	<Integer>	Read-only	.
activepolicy	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditnslogpolicy_tmglobal_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ auditnslogpolicy_tmglobal_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of auditnslogpolicy_tmglobal_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/auditnslogpolicy_tmglobal_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the auditnslogpolicy_tmglobal_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "auditnslogpolicy_tmglobal_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"priority":<Integer_value>,
```

```
"activepolicy":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditnslogpolicy_tmglobal_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/auditnslogpolicy_tmglobal_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "auditnslogpolicy_tmglobal_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"priority":<Integer_value>,

"activepolicy":<Integer_value>
```

```
}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditnslogpolicy_tmglobal_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"auditnslogpolicy_tmglobal_binding": [ { "__count": "#no"} ] }
```

auditnslogpolicy_vpnglobal_binding

Binding object showing the vpnglobal that can be bound to auditnslogpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
boundto	<String>	Read-write	The entity name to which policy is bound.
name	<String>	Read-write	Name of the policy. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
activepolicy	<Integer>	Read-only	.
priority	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditnslogpolicy_vpnglobal_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ auditnslogpolicy_vpnglobal_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of auditnslogpolicy_vpnglobal_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/auditnslogpolicy_vpnglobal_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the auditnslogpolicy_vpnglobal_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "auditnslogpolicy_vpnglobal_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"activepolicy":<Integer_value>,

"priority":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditnslogpolicy_vpnglobal_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/auditnslogpolicy_vpnglobal_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "auditnslogpolicy_vpnglobal_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"activepolicy":<Integer_value>,

"priority":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditnslogpolicy_vpnglobal_binding/name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"auditnslogpolicy_vpnglobal_binding": [ { "__count": "#no"} ] }
```

auditnslogpolicy_vpnvserver_binding

Binding object showing the vpnvserver that can be bound to auditnslogpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the policy. Minimum length = 1
boundto	<String>	Read-write	The entity name to which policy is bound.
activepolicy	<Integer>	Read-only	.
priority	<Integer>	Read-only	.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditnslogpolicy_vpnvserver_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ auditnslogpolicy_vpnvserver_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of auditnslogpolicy_vpnvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/auditnslogpolicy_vpnvserver_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the auditnslogpolicy_vpnvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "auditnslogpolicy_vpnvserver_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"activepolicy":<Integer_value>,

"priority":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditnslogpolicy_vpnvserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/auditnslogpolicy_vpnvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "auditnslogpolicy_vpnvserver_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"activepolicy":<Integer_value>,

"priority":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditnslogpolicy_vpnvserver_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"auditnslogpolicy_vpnvserver_binding": [ { "__count": "#no"} ] }
```

auditsyslogaction

Configuration for system log action resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the syslog action. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@),

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			equals (=), colon (:), and underscore characters. Cannot be changed after the syslog action is added. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my syslog action" or 'my syslog action'). Minimum length = 1
serverip	<String>	Read-write	IP address of the syslog server. Minimum length = 1
serverdomainname	<String>	Read-write	SYSLOG server name as a FQDN. Mutually exclusive with serverIP/ lbVserverName. Minimum length = 1 Maximum length = 255
domainresolveretry	<Integer>	Read-write	Time, in seconds, for which the Citrix ADC waits before sending

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			another DNS query to resolve the host name of the syslog server if the last query failed. Default value: 5 Minimum value = 5 Maximum value = 20939
lbvservername	<String>	Read-write	Name of the LB vserver. Mutually exclusive with syslog serverIP/ serverName. Minimum length = 1 Maximum length = 127
serverport	<Integer>	Read-write	Port on which the syslog server accepts connections. Minimum value = 1
loglevel	<String[]>	Read-write	Audit log level, which specifies the types of events to log. Available values function as follows: * ALL - All events. * EMERGENCY - Events that indicate an immediate crisis on the server.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			* ALERT - Events that might require action. * CRITICAL - Events that indicate an imminent server crisis. * ERROR - Events that indicate some type of error. * WARNING - Events that require action in the near future. * NOTICE - Events that the administrator should know about. * INFORMATIONAL - All but low-level events. * DEBUG - All events, in extreme detail. * NONE - No events. Possible values = ALL, EMERGENCY, ALERT, CRITICAL, ERROR, WARNING,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			NOTICE, INFORMATIONAL, DEBUG, NONE
managementlog	<String[]>	Read-write	Management log specifies the categories of log files to be exported. It use destination and transport from PE params. Available values function as follows: * ALL - All categories (SHELL, NSMGMT and ACCESS). * SHELL - bash.log, and sh.log. * ACCESS - auth.log, nsvpn.log, httpaccess.log, httperror.log, httpaccess-vpn.log and httperror-vpn.log. * NSMGMT - notice.log and ns.log. * NONE - No logs. Possible values = ALL, SHELL,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			ACCESS, NSMGMT, NONE
mgmtloglevel	<String[]>	Read-write	Management log level, which specifies the types of events to log. Available values function as follows: * ALL - All events. * EMERGENCY - Events that indicate an immediate crisis on the server. * ALERT - Events that might require action. * CRITICAL - Events that indicate an imminent server crisis. * ERROR - Events that indicate some type of error. * WARNING - Events that require action in the near future. * NOTICE - Events that the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			administrator should know about. * INFORMATIONAL - All but low-level events. * DEBUG - All events, in extreme detail. * NONE - No events. Possible values = ALL, EMERGENCY, ALERT, CRITICAL, ERROR, WARNING, NOTICE, INFORMATIONAL, DEBUG, NONE
syslogcompliance	<String>	Read-write	Setting this parameter ensures that all the Audit Logs generated for this Syslog Action comply with an RFC. For example, set it to RFC5424 to ensure RFC 5424 compliance. Possible values = RFC5424
dateformat	<String>	Read-write	Format of dates in the logs.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Supported formats are: * MMDDYYYY. -U.S. style month/date/year format. * DDMMYYYY - European style date/month/year format. * YYYYMMDD - ISO style year/month/date format. Possible values = MMDDYYYY, DDMMYYYY, YYYYMMDD
logfacility	<String>	Read-write	Facility value, as defined in RFC 3164, assigned to the log message. Log facility values are numbers 0 to 7 (LOCAL0 through LOCAL7). Each number indicates where a specific message originated from, such as the Citrix ADC itself, the VPN, or external. Possible values = LOCAL0, LOCAL1, LOCAL2, LOCAL3,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			LOCAL4, LOCAL5, LOCAL6, LOCAL7
tcp	<String>	Read-write	Log TCP messages. Possible values = NONE, ALL
acl	<String>	Read-write	Log access control list (ACL) messages. Possible values = ENABLED, DISABLED
timezone	<String>	Read-write	Time zone used for date and timestamps in the logs. Supported settings are: * GMT_TIME. Coordinated Universal time. * LOCAL_TIME. Use the server's timezone setting. Possible values = GMT_TIME, LOCAL_TIME
userdefinedauditlog	<String>	Read-write	Log user-configurable log messages to syslog. Setting this parameter to NO causes auditing to ignore all user-configured message

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			actions. Setting this parameter to YES causes auditing to log user-configured message actions that meet the other logging criteria. Possible values = YES, NO
appflowexport	<String>	Read-write	Export log messages to AppFlow collectors. Appflow collectors are entities to which log messages can be sent so that some action can be performed on them. Possible values = ENABLED, DISABLED
lsn	<String>	Read-write	Log lsn info. Possible values = ENABLED, DISABLED
alg	<String>	Read-write	Log alg info. Possible values = ENABLED, DISABLED
subscriberlog	<String>	Read-write	Log subscriber session event information.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ENABLED, DISABLED
transport	<String>	Read-write	Transport type used to send auditlogs to syslog server. Default type is UDP. Possible values = TCP, UDP, HTTP
httpauthtoken	<String>	Read-write	Token for authenticating with the endpoint. If the endpoint requires the Authorization header in a particular format, specify the complete format as the value to this parameter. For eg., in case of splunk, the Authorization header is required to be of the form - Splunk <auth-token>. Maximum length = 256
httpendpointurl	<String>	Read-write	The URL at which to upload the logs messages on the endpoint. Maximum length = 256
httpschemafile	<String>	Read-write	HTTP Schema file to input tokens to be sent in log message to log server.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum length = 256
tcpprofilename	<String>	Read-write	Name of the TCP profile whose settings are to be applied to the audit server info to tune the TCP connection parameters. Minimum length = 1 Maximum length = 127
maxlogdatasizetohold	<Integer>	Read-write	Max size of log data that can be held in NSB chain of server info. Default value: 500 Minimum value = 50 Maximum value = 25600
dns	<String>	Read-write	Log DNS related syslog messages. Possible values = ENABLED, DISABLED
contentinspectionlog	<String>	Read-write	Log Content Inspection event information. Possible values = ENABLED, DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
netprofile	<String>	Read-write	Name of the network profile. The SNIP configured in the network profile will be used as source IP while sending log messages. Minimum length = 1 Maximum length = 127
sslinterception	<String>	Read-write	Log SSL Interception event information. Possible values = ENABLED, DISABLED
urlfiltering	<String>	Read-write	Log URL filtering event information. Possible values = ENABLED, DISABLED
streamanalytics	<String>	Read-write	Export log stream analytics statistics to syslog server. Possible values = ENABLED, DISABLED
protocolviolations	<String>	Read-write	Log protocol violations. Possible values = ALL, NONE

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
denylistviolations	<String>	Read-write	Log denylist violations. Possible values = ENABLED, DISABLED
domainresolvenow	<Boolean>	Read-write	Immediately send a DNS query to resolve the server's domain name.
ip	<String>	Read-only	The resolved IP address of the syslog server.
builtin	<String[]>	Read-only	Indicates that a variable is a built-in (SYSTEM INTERNAL) type. Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL
feature	<String>	Read-only	The feature to be checked while applying this config.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE

- UNSET
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditsyslogaction **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"auditsyslogaction":{

<b>"name":<String_value>,

</b>"serverip":<String_value>,

"serverdomainname":<String_value>,

"domainresolveretry":<Integer_value>,

"lbvservername":<String_value>,

"serverport":<Integer_value>,

<b>"loglevel":<String[]_value>,

</b>"managementlog":<String[]_value>,

"mgmtloglevel":<String[]_value>,

"syslogcompliance":<String_value>,

"dateformat":<String_value>,

"logfacility":<String_value>,

"tcp":<String_value>,

"acl":<String_value>,

"timezone":<String_value>,

"userdefinedauditlog":<String_value>,

"appflowexport":<String_value>,

"lsn":<String_value>,

"alg":<String_value>,

"subscriberlog":<String_value>,

"transport":<String_value>,
```

```
"httpauthtoken":<String_value>,

"httpendpointurl":<String_value>,

"httpschemafile":<String_value>,

"tcpprofilename":<String_value>,

"maxlogdatasizetohold":<Integer_value>,

"dns":<String_value>,

"contentinspectionlog":<String_value>,

"netprofile":<String_value>,

"sslinterception":<String_value>,

"urlfiltering":<String_value>,

"streamanalytics":<String_value>,

"protocolviolations":<String_value>,

"denylistviolations":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditsyslogaction/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditsyslogaction **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"auditsyslogaction":{

<b>"name":<String_value>,

</b>"serverip":<String_value>,

"serverdomainname":<String_value>,

"lbvservername":<String_value>,

"domainresolveretry":<Integer_value>,

"domainresolvenow":<Boolean_value>,

"serverport":<Integer_value>,

"loglevel":<String[]_value>,

"managementlog":<String[]_value>,

"mgmtloglevel":<String[]_value>,

"syslogcompliance":<String_value>,

"dateformat":<String_value>,

"logfacility":<String_value>,

"tcp":<String_value>,
```

```
"acl":<String_value>,

"timezone":<String_value>,

"userdefinedauditlog":<String_value>,

"appflowexport":<String_value>,

"lsn":<String_value>,

"alg":<String_value>,

"subscriberlog":<String_value>,

"httpauthtoken":<String_value>,

"httpendpointurl":<String_value>,

"httpschemafile":<String_value>,

"tcpprofilename":<String_value>,

"maxlogdatasizetohold":<Integer_value>,

"dns":<String_value>,

"contentinspectionlog":<String_value>,

"netprofile":<String_value>,

"sslinterception":<String_value>,

"urlfiltering":<String_value>,

"streamanalytics":<String_value>,

"protocolviolations":<String_value>,

"denylistviolations":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditsyslogaction? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"auditsyslogaction":{

<b>"name":<String_value>,

</b>"serverport":true,

"loglevel":true,

"dateformat":true,

"logfacility":true,

"tcp":true,

"acl":true,

"timezone":true,

"userdefinedauditlog":true,

"appflowexport":true,

"lsn":true,
```

```
"alg":true,

"subscriberlog":true,

"tcpprofilename":true,

"maxlogdatasizetohold":true,

"dns":true,

"contentinspectionlog":true,

"netprofile":true,

"sslinterception":true,

"urlfiltering":true,

"streamanalytics":true,

"httpauthtoken":true,

"httpendpointurl":true,

"httpschemafile":true,

"protocolviolations":true,

"denylistviolations":true,

"managementlog":true,

"mgmtloglevel":true,

"syslogcompliance":true

}}
```


Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditsyslogaction **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/auditsyslogaction? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/auditsyslogaction? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of auditsyslogaction resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/auditsyslogaction? **view=summary**

Use this query-parameter to get the summary output of auditsyslogaction resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/auditsyslogaction? **pagesize=#no;pageno=#no**

Use this query-parameter to get the auditsyslogaction resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "auditsyslogaction": [ {

"name":<String_value>,

"serverip":<String_value>,

"serverdomainname":<String_value>,

"ip":<String_value>,

"lbvservername":<String_value>,

"domainresolveretry":<Integer_value>,

"domainresolvenow":<Boolean_value>,

"serverport":<Integer_value>,

"loglevel":<String[]_value>,

"managementlog":<String[]_value>,

"mgmtloglevel":<String[]_value>,

"syslogcompliance":<String_value>,

"dateformat":<String_value>,

"logfacility":<String_value>,

"tcp":<String_value>,

"acl":<String_value>,

"timezone":<String_value>,

"userdefinedauditlog":<String_value>,

"appflowexport":<String_value>,

"builtin":<String[]_value>,
```

```
"feature":<String_value>,

"lsn":<String_value>,

"alg":<String_value>,

"subscriberlog":<String_value>,

"transport":<String_value>,

"httpauthtoken":<String_value>,

"httpendpointurl":<String_value>,

"httpschemafile":<String_value>,

"tcpprofilename":<String_value>,

"maxlogdatasizetohold":<Integer_value>,

"dns":<String_value>,

"netprofile":<String_value>,

"sslinterception":<String_value>,

"urlfiltering":<String_value>,

"contentinspectionlog":<String_value>,

"streamanalytics":<String_value>,

"protocolviolations":<String_value>,

"denylistviolations":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditsyslogaction/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/auditsyslogaction/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/auditsyslogaction/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of auditsyslogaction resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "auditsyslogaction": [ {

"name":<String_value>,

"serverip":<String_value>,

"serverdomainname":<String_value>,

"ip":<String_value>,
```

```
"lbvservername":<String_value>,

"domainresolveretry":<Integer_value>,

"domainresolvenow":<Boolean_value>,

"serverport":<Integer_value>,

"loglevel":<String[]_value>,

"managementlog":<String[]_value>,

"mgmtloglevel":<String[]_value>,

"syslogcompliance":<String_value>,

"dateformat":<String_value>,

"logfacility":<String_value>,

"tcp":<String_value>,

"acl":<String_value>,

"timezone":<String_value>,

"userdefinedauditlog":<String_value>,

"appflowexport":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"lsn":<String_value>,

"alg":<String_value>,

"subscriberlog":<String_value>,

"transport":<String_value>,

"httpauthtoken":<String_value>,
```

```
"httpendpointurl":<String_value>,

"httpschemafile":<String_value>,

"tcpprofilename":<String_value>,

"maxlogdatasizetohold":<Integer_value>,

"dns":<String_value>,

"netprofile":<String_value>,

"sslinterception":<String_value>,

"urlfiltering":<String_value>,

"contentinspectionlog":<String_value>,

"streamanalytics":<String_value>,

"protocolviolations":<String_value>,

"denylistviolations":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditsyslogaction? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "auditsyslogaction": [ { "__count": "#no"} ] }
```

auditsyslogglobal_auditsyslogpolicy_binding

Binding object showing the auditsyslogpolicy that can be bound to auditsyslogglobal.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
feature	<String>	Read-write	The feature to be checked while applying this config.
globalbindtype	<String>	Read-write	. Default value: SYSTEM_GLOBAL Possible values = SYSTEM_GLOBAL, VPN_GLOBAL, RNAT_GLOBAL, APPFW_GLOBAL, TM_GLOBAL
policyname	<String>	Read-write	Name of the audit syslog policy.
builtin	<String[]>	Read-write	Indicates that a variable is a built-in

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			(SYSTEM INTERNAL) type. Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL
priority	<Integer>	Read-write	Specifies the priority of the policy. Minimum value = 1 Maximum value = 2147483647
numpol	<Integer>	Read-only	number of polices bound to label.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/auditsyslogglobal_auditsyslogpolicy_binding
HTTP Method: PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"auditsyslogglobal_auditsyslogpolicy_binding":{

<b>"policyname":<String_value>,

</b><b>"priority":<Integer_value>,

</b>"globalbindtype":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditsyslogglobal_auditsyslogpolicy_binding **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/auditsyslogglobal_auditsyslogpolicy_binding? **args=policyname: <String_value> ,globalbindtype: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditsyslogglobal_auditsyslogpolicy_binding **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/auditsyslogglobal_auditsyslogpolicy_binding? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of auditsyslogglobal_auditsyslogpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/auditsyslogglobal_auditsyslogpolicy_binding? **pagesize=#no;pageno=#no**

Use this query-parameter to get the auditsyslogglobal_auditsyslogpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "auditsyslogglobal_auditsyslogpolicy_binding": [ {

"feature":<String_value>,

"globalbindtype":<String_value>,

"policyname":<String_value>,

"builtin":<String[]_value>,

"priority":<Integer_value>,

"numpol":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditsyslogglobal_auditsyslogpolicy_binding?**count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "auditsysloglobal_auditsyslogpolicy_binding": [ { "__count": "#no"} ] }
```

auditsysloglobal_binding

Binding object which returns the resources bound to auditsysloglobal.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
auditsysloglobal_auditsyslogpolicy_binding	<auditsysloglobal_auditsyslogpolicy_binding[]>	Read-write	auditsyslogpolicy that can be bound to auditsysloglobal.

Operations

(click to see Properties)

- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditsyslogglobal_binding

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "auditsyslogglobal_binding": [ {

"auditsyslogglobal_auditsyslogpolicy_binding":<auditsyslogglobal_auditsyslogpolicy_binding[]_value>

}]}
```

auditsyslogparams

Configuration for system log parameters resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
serverip	<String>	Read-write	IP address of the syslog server. Minimum length = 1
serverport	<Integer>	Read-write	Port on which the syslog server accepts connections. Minimum value = 1
dateformat	<String>	Read-write	Format of dates in the logs. Supported formats are: * MMDDYYYY - U.S. style month/ date/year format. * DDMMYYYY. European style -date/month/year format. * YYYYMMDD - ISO style year/ month/date format. Possible values = MMDDYYYY, DDMMYYYY, YYYYMMDD

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
loglevel	<String[]>	Read-write	Types of information to be logged. Available settings function as follows: * ALL - All events. * EMERGENCY - Events that indicate an immediate crisis on the server. * ALERT - Events that might require action. * CRITICAL - Events that indicate an imminent server crisis. * ERROR - Events that indicate some type of error. * WARNING - Events that require action in the near future. * NOTICE - Events that the administrator should know about. * INFORMATIONAL - All but low-level events.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			* NONE - No events. Possible values = ALL, EMERGENCY, ALERT, CRITICAL, ERROR, WARNING, NOTICE, INFORMATIONAL, NONE
logfacility	<String>	Read-write	Facility value, as defined in RFC 3164, assigned to the log message. Log facility values are numbers 0 to 7 (LOCAL0 through LOCAL7). Each number indicates where a specific message originated from, such as the Citrix ADC itself, the VPN, or external. Possible values = LOCAL0, LOCAL1, LOCAL2, LOCAL3, LOCAL4, LOCAL5, LOCAL6, LOCAL7
tcp	<String>	Read-write	Log TCP messages. Possible values = NONE, ALL

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
acl	<String>	Read-write	Log access control list (ACL) messages. Possible values = ENABLED, DISABLED
timezone	<String>	Read-write	Time zone used for date and timestamps in the logs. Available settings function as follows: * GMT_TIME - Coordinated Universal Time. * LOCAL_TIME Use the server's timezone setting. Possible values = GMT_TIME, LOCAL_TIME
userdefinedauditlog	<String>	Read-write	Log user-configurable log messages to syslog. Setting this parameter to NO causes audit to ignore all user-configured message actions. Setting this parameter to YES causes audit to log user-configured message actions

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			that meet the other logging criteria. Possible values = YES, NO
appflowexport	<String>	Read-write	Export log messages to AppFlow collectors. Appflow collectors are entities to which log messages can be sent so that some action can be performed on them. Possible values = ENABLED, DISABLED
lsn	<String>	Read-write	Log the LSN messages. Possible values = ENABLED, DISABLED
alg	<String>	Read-write	Log the ALG messages. Possible values = ENABLED, DISABLED
subscriberlog	<String>	Read-write	Log subscriber session event information. Possible values = ENABLED, DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
dns	<String>	Read-write	Log DNS related syslog messages. Possible values = ENABLED, DISABLED
sslinterception	<String>	Read-write	Log SSL Interceptionn event information. Possible values = ENABLED, DISABLED
urlfiltering	<String>	Read-write	Log URL filtering event information. Possible values = ENABLED, DISABLED
contentinspectionlog	<String>	Read-write	Log Content Inspection event ifnormation. Possible values = ENABLED, DISABLED
streamanalytics	<String>	Read-write	Export log stream analytics statistics to syslog server. Possible values = ENABLED, DISABLED
protocolviolations	<String>	Read-write	Log protocol violations. Possible values = ALL, NONE

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
denylistviolations	<String>	Read-write	Log denylist violations. Possible values = ENABLED, DISABLED
builtin	<String[]>	Read-only	Indicates that a variable is a built-in (SYSTEM INTERNAL) type. Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL
feature	<String>	Read-only	The feature to be checked while applying this config.
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- UPDATE
- UNSET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditsyslogparams **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"auditsyslogparams":{

"serverip":<String_value>,

"serverport":<Integer_value>,

"dateformat":<String_value>,

"loglevel":<String[]_value>,

"logfacility":<String_value>,

"tcp":<String_value>,

"acl":<String_value>,
```

```
"timezone":<String_value>,

"userdefinedauditlog":<String_value>,

"appflowexport":<String_value>,

"lsn":<String_value>,

"alg":<String_value>,

"subscriberlog":<String_value>,

"dns":<String_value>,

"sslinterception":<String_value>,

"urlfiltering":<String_value>,

"contentinspectionlog":<String_value>,

"streamanalytics":<String_value>,

"protocolviolations":<String_value>,

"denylistviolations":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditsyslogparams? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"auditsyslogparams":{

"serverip":true,

"serverport":true,

"loglevel":true,

"dateformat":true,

"logfacility":true,

"tcp":true,

"acl":true,

"timezone":true,

"userdefinedauditlog":true,

"appflowexport":true,

"lsn":true,

"alg":true,

"subscriberlog":true,

"dns":true,

"contentinspectionlog":true,

"sslinterception":true,

"urlfiltering":true,

"streamanalytics":true,

"protocolviolations":true,

"denylistviolations":true
```

```
}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditsyslogparams **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "auditsyslogparams": [ {

"name":<String_value>,

"serverip":<String_value>,

"serverport":<Integer_value>,

"dateformat":<String_value>,

"loglevel":<String[]_value>,

"logfacility":<String_value>,

"tcp":<String_value>,
```

```
"acl":<String_value>,

"timezone":<String_value>,

"userdefinedauditlog":<String_value>,

"appflowexport":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"lsn":<String_value>,

"alg":<String_value>,

"subscriberlog":<String_value>,

"dns":<String_value>,

"sslinterception":<String_value>,

"urlfiltering":<String_value>,

"contentinspectionlog":<String_value>,

"streamanalytics":<String_value>,

"protocolviolations":<String_value>,

"denylistviolations":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

auditsyslogpolicy

Configuration for system log policy resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the policy. Must begin with a letter, number, or the underscore character (_), and must consist only of letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore characters. Cannot be changed after the syslog policy is added. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my syslog policy" or 'my syslog policy'). Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
rule	<String>	Read-write	Name of the Citrix ADC named rule, or an expression, that defines the messages to be logged to the syslog server. Minimum length = 1
action	<String>	Read-write	Syslog server action to perform when this policy matches traffic. NOTE: A syslog server action must be associated with a syslog audit policy. Minimum length = 1
builtin	<String[]>	Read-only	Indicates that a variable is a built-in (SYSTEM INTERNAL) type. Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL
feature	<String>	Read-only	The feature to be checked while applying this config.
expressiontype	<String>	Read-only	Type of policy (Classic/Advanced).

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = Classic Policy, Advanced Policy
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditsyslogpolicy **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"auditsyslogpolicy":{

<b>"name":<String_value>,

</b><b>"rule":<String_value>,

</b><b>"action":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditsyslogpolicy/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditsyslogpolicy **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"auditsyslogpolicy":{

<b>"name":<String_value>,

</b>"rule":<String_value>,

"action":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditsyslogpolicy **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/auditsyslogpolicy? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/auditsyslogpolicy? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of auditsyslogpolicy resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/auditsyslogpolicy? **view=summary**

Use this query-parameter to get the summary output of auditsyslogpolicy resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/auditsyslogpolicy? **pagesize=#no;pageno=#no**

Use this query-parameter to get the auditsyslogpolicy resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "auditsyslogpolicy": [ {

"name":<String_value>,

"rule":<String_value>,

"action":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"expressiontype":<String_value>,
```

```
"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditsyslogpolicy/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/auditsyslogpolicy/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/auditsyslogpolicy/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of auditsyslogpolicy resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "auditsyslogpolicy": [ {

"name":<String_value>,
```

```
"rule":<String_value>,

"action":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"expressiontype":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditsyslogpolicy? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "auditsyslogpolicy": [ { "__count": "#no"} ] }
```

auditsyslogpolicy_aaagroup_binding

Binding object showing the aaagroup that can be bound to auditsyslogpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the policy. Minimum length = 1
boundto	<String>	Read-write	The entity name to which policy is bound.
priority	<Integer>	Read-only	.
activepolicy	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.
- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditsyslogpolicy_aaagroup_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ auditsyslogpolicy_aaagroup_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of auditsyslogpolicy_aaagroup_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/auditsyslogpolicy_aaagroup_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the auditsyslogpolicy_aaagroup_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "auditsyslogpolicy_aaagroup_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"priority":<Integer_value>,

"activepolicy":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditsyslogpolicy_aaagroup_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/auditsyslogpolicy_aaagroup_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "auditsyslogpolicy_aaagroup_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"priority":<Integer_value>,

"activepolicy":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditsyslogpolicy_aaagroup_binding/name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"auditsyslogpolicy_aaagroup_binding": [ { "__count": "#no"} ] }
```

auditsyslogpolicy_aaauser_binding

Binding object showing the aaauser that can be bound to auditsyslogpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the policy. Minimum length = 1
boundto	<String>	Read-write	The entity name to which policy is bound.
activepolicy	<Integer>	Read-only	.
priority	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditsyslogpolicy_aaauser_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ auditsyslogpolicy_aaauser_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of auditsyslogpolicy_aaauser_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/auditsyslogpolicy_aaauser_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the auditsyslogpolicy_aaauser_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "auditsyslogpolicy_aaauser_binding": [ {

"name":<String_value>,
```

```
"boundto":<String_value>,

"activepolicy":<Integer_value>,

"priority":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditsyslogpolicy_aaauser_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/auditsyslogpolicy_aaauser_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "auditsyslogpolicy_aaauser_binding": [ {

"name":<String_value>,

"boundto":<String_value>,
```

```
"activepolicy":<Integer_value>,

"priority":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditsyslogpolicy_aaauser_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"auditsyslogpolicy_aaauser_binding": [ { "__count": "#no"} ] }
```

auditsyslogpolicy_auditsyslogglobal_binding

Binding object showing the auditsyslogglobal that can be bound to auditsyslogpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the policy. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
boundto	<String>	Read-write	The entity name to which policy is bound.
priority	<Integer>	Read-only	.
activepolicy	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditsyslogpolicy_auditsyslogglobal_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ auditsyslogpolicy_auditsyslogglobal_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of auditsyslogpolicy_auditsyslogglobal_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ auditsyslogpolicy_auditsyslogglobal_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the auditsyslogpolicy_auditsyslogglobal_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "auditsyslogpolicy_auditsyslogglobal_binding": [ {

"name":<String_value>,

"boundto":<String_value>,
```

```
"priority":<Integer_value>,

"activepolicy":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditsyslogpolicy_auditsyslogglobal_binding
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/auditsyslogpolicy_auditsyslogglobal_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "auditsyslogpolicy_auditsyslogglobal_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"priority":<Integer_value>,
```

```
"activepolicy":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditsyslogpolicy_auditsyslogglobal_binding/name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"auditsyslogpolicy_auditsyslogglobal_binding": [ { "__count": "#no"} ] }
```

auditsyslogpolicy_authenticationvserver_binding

Binding object showing the authenticationvserver that can be bound to auditsyslogpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the policy. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
boundto	<String>	Read-write	The entity name to which policy is bound.
activepolicy	<Integer>	Read-only	.
priority	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/ auditsyslogpolicy_authenticationvserver_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/auditsyslogpolicy_authenticationvserver_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of auditsyslogpolicy_authenticationvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ auditsyslogpolicy_authenticationvserver_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the auditsyslogpolicy_authenticationvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "auditsyslogpolicy_authenticationvserver_binding": [ {

"name":<String_value>,
```

```
"boundto":<String_value>,

"activepolicy":<Integer_value>,

"priority":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/ auditsyslogpolicy_authenticationvserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ auditsyslogpolicy_authenticationvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "auditsyslogpolicy_authenticationvserver_binding": [ {

"name":<String_value>,

"boundto":<String_value>,
```

```
"activepolicy":<Integer_value>,

"priority":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/ auditsyslogpolicy_authenticationvserver_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"auditsyslogpolicy_authenticationvserver_binding": [ { "__count":
"#no"} ] }
```

auditsyslogpolicy_binding

Binding object which returns the resources bound to auditsyslogpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the policy. Minimum length = 1
auditsyslogpolicy_lbvserver_binding	<auditsyslogpolicy_lbvserver_binding[]>	Read-only	lbvserver that can be bound to auditsyslogpolicy.
auditsyslogpolicy_auditsysloglobal_binding	<auditsyslogpolicy_auditsysloglobal_binding[]>	Read-only	auditsysloglobal that can be bound to auditsyslogpolicy.
auditsyslogpolicy_aaauser_binding	<auditsyslogpolicy_aaauser_binding[]>	Read-only	aaauser that can be bound to auditsyslogpolicy.
auditsyslogpolicy_authenticationvserver_binding	<auditsyslogpolicy_authenticationvserver_binding[]>	Read-only	authenticationvserver that can be bound to auditsyslogpolicy.
auditsyslogpolicy_rnatglobal_binding	<auditsyslogpolicy_rnatglobal_binding[]>	Read-only	rnatglobal that can be bound to auditsyslogpolicy.
auditsyslogpolicy_systemglobal_binding	<auditsyslogpolicy_systemglobal_binding[]>	Read-only	systemglobal that can be bound to auditsyslogpolicy.
auditsyslogpolicy_tmglobal_binding	<auditsyslogpolicy_tmglobal_binding[]>	Read-only	tmglobal that can be bound to auditsyslogpolicy.
auditsyslogpolicy_aaagroup_binding	<auditsyslogpolicy_aaagroup_binding[]>	Read-only	aaagroup that can be bound to auditsyslogpolicy.
auditsyslogpolicy_vpnglobal_binding	<auditsyslogpolicy_vpnglobal_binding[]>	Read-only	vpnglobal that can be bound to auditsyslogpolicy.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
auditsyslogpolicy_vpnvserver_binding	<auditsyslogpolicy_vpnvserver_binding[]>	Read-only	vpnvserver that can be bound to auditsyslogpolicy.
auditsyslogpolicy_csvserver_binding	<auditsyslogpolicy_csvserver_binding[]>	Read-only	csvserver that can be bound to auditsyslogpolicy.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditsyslogpolicy_binding/ name_value<String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "auditsyslogpolicy_binding": [ {

"name":<String_value>,

"auditsyslogpolicy_vpnvserver_binding":<auditsyslogpolicy_vpnvserver_bindi
ng[]_value>,

"auditsyslogpolicy_rnatglobal_binding":<auditsyslogpolicy_rnatglobal_bindi
ng[]_value>,

"auditsyslogpolicy_auditsyslogglobal_binding":<auditsyslogpolicy_auditsysl
ogglobal_binding[]_value>,

"auditsyslogpolicy_authenticationvserver_binding":<auditsyslogpolicy_authe
nticationvserver_binding[]_value>,

"auditsyslogpolicy_aaauser_binding":<auditsyslogpolicy_aaauser_binding[]_v
alue>,

"auditsyslogpolicy_vpnglobal_binding":<auditsyslogpolicy_vpnglobal_binding
[]_value>,
```

```
"auditsyslogpolicy_aaagroup_binding":<auditsyslogpolicy_aaagroup_binding[]
_value>,

"auditsyslogpolicy_csvserver_binding":<auditsyslogpolicy_csvserver_binding
[]_value>,

"auditsyslogpolicy_tmglobal_binding":<auditsyslogpolicy_tmglobal_binding[]
_value>,

"auditsyslogpolicy_lbvserver_binding":<auditsyslogpolicy_lbvserver_binding
[]_value>,

"auditsyslogpolicy_systemglobal_binding":<auditsyslogpolicy_systemglobal_b
inding[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditsyslogpolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/auditsyslogpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "auditsyslogpolicy_binding": [ {

"name":<String_value>,

"auditsyslogpolicy_vpnvserver_binding":<auditsyslogpolicy_vpnvserver_binding[]_value>,

"auditsyslogpolicy_rnatglobal_binding":<auditsyslogpolicy_rnatglobal_binding[]_value>,

"auditsyslogpolicy_auditsyslogglobal_binding":<auditsyslogpolicy_auditsyslogglobal_binding[]_value>,

"auditsyslogpolicy_authenticationvserver_binding":<auditsyslogpolicy_authenticationvserver_binding[]_value>,

"auditsyslogpolicy_aaauser_binding":<auditsyslogpolicy_aaauser_binding[]_value>,

"auditsyslogpolicy_vpnglobal_binding":<auditsyslogpolicy_vpnglobal_binding[]_value>,

"auditsyslogpolicy_aaagroup_binding":<auditsyslogpolicy_aaagroup_binding[]_value>,

"auditsyslogpolicy_csvserver_binding":<auditsyslogpolicy_csvserver_binding[]_value>,

"auditsyslogpolicy_tmglobal_binding":<auditsyslogpolicy_tmglobal_binding[]_value>,

"auditsyslogpolicy_lbvserver_binding":<auditsyslogpolicy_lbvserver_binding[]_value>,

"auditsyslogpolicy_systemglobal_binding":<auditsyslogpolicy_systemglobal_binding[]_value>

}]}
```

auditsyslogpolicy_csvserver_binding

Binding object showing the csvserver that can be bound to auditsyslogpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
boundto	<String>	Read-write	The entity name to which policy is bound.
name	<String>	Read-write	Name of the policy. Minimum length = 1
priority	<Integer>	Read-only	.
activepolicy	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.
- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of

creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditsyslogpolicy_csvserver_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ auditsyslogpolicy_csvserver_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of auditsyslogpolicy_csvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/auditsyslogpolicy_csvserver_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the auditsyslogpolicy_csvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "auditsyslogpolicy_csvserver_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"priority":<Integer_value>,

"activepolicy":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditsyslogpolicy_csvserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/auditsyslogpolicy_csvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "auditsyslogpolicy_csvserver_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"priority":<Integer_value>,

"activepolicy":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditsyslogpolicy_csvserver_binding/name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"auditsyslogpolicy_csvserver_binding": [ { "__count": "#no"} ] }
```

auditsyslogpolicy_lbvserver_binding

Binding object showing the lbvserver that can be bound to auditsyslogpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
boundto	<String>	Read-write	The entity name to which policy is bound.
name	<String>	Read-write	Name of the policy. Minimum length = 1
activepolicy	<Integer>	Read-only	.
priority	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditsyslogpolicy_lbvserver_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ auditsyslogpolicy_lbvserver_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of auditsyslogpolicy_lbvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/auditsyslogpolicy_lbvserver_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the auditsyslogpolicy_lbvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "auditsyslogpolicy_lbvserver_binding": [ {

"boundto":<String_value>,
```

```
"name":<String_value>,

"activepolicy":<Integer_value>,

"priority":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditsyslogpolicy_lbvserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/auditsyslogpolicy_lbvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "auditsyslogpolicy_lbvserver_binding": [ {

"boundto":<String_value>,

"name":<String_value>,
```

```
"activepolicy":<Integer_value>,

"priority":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditsyslogpolicy_lbvserver_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"auditsyslogpolicy_lbvserver_binding": [ { "__count": "#no"} ] }
```

auditsyslogpolicy_rnatglobal_binding

Binding object showing the rnatglobal that can be bound to auditsyslogpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the policy. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
boundto	<String>	Read-write	The entity name to which policy is bound.
priority	<Integer>	Read-only	.
activepolicy	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditsyslogpolicy_rnatglobal_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ auditsyslogpolicy_rnatglobal_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of auditsyslogpolicy_rnatglobal_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/auditsyslogpolicy_rnatglobal_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the auditsyslogpolicy_rnatglobal_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "auditsyslogpolicy_rnatglobal_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"priority":<Integer_value>,
```

```
"activepolicy":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditsyslogpolicy_rnatglobal_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/auditsyslogpolicy_rnatglobal_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "auditsyslogpolicy_rnatglobal_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"priority":<Integer_value>,

"activepolicy":<Integer_value>
```

```
}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditsyslogpolicy_rnatglobal_binding/name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"auditsyslogpolicy_rnatglobal_binding": [ { "__count": "#no"} ] }
```

auditsyslogpolicy_systemglobal_binding

Binding object showing the systemglobal that can be bound to auditsyslogpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the policy. Minimum length = 1
boundto	<String>	Read-write	The entity name to which policy is bound.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
priority	<Integer>	Read-only	.
activepolicy	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditsyslogpolicy_systemglobal_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ auditsyslogpolicy_systemglobal_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of auditsyslogpolicy_systemglobal_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/auditsyslogpolicy_systemglobal_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the auditsyslogpolicy_systemglobal_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "auditsyslogpolicy_systemglobal_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"priority":<Integer_value>,

"activepolicy":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditsyslogpolicy_systemglobal_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/auditsyslogpolicy_systemglobal_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "auditsyslogpolicy_systemglobal_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"priority":<Integer_value>,

"activepolicy":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditsyslogpolicy_systemglobal_binding/name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"auditsyslogpolicy_systemglobal_binding": [ { "__count": "#no"} ] }
```

auditsyslogpolicy_tmglobal_binding

Binding object showing the tmglobal that can be bound to auditsyslogpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
boundto	<String>	Read-write	The entity name to which policy is bound.
name	<String>	Read-write	Name of the policy. Minimum length = 1
activepolicy	<Integer>	Read-only	.
priority	<Integer>	Read-only	.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditsyslogpolicy_tmglobal_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ auditsyslogpolicy_tmglobal_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of auditsyslogpolicy_tmglobal_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/auditsyslogpolicy_tmglobal_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the auditsyslogpolicy_tmglobal_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "auditsyslogpolicy_tmglobal_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"activepolicy":<Integer_value>,

"priority":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditsyslogpolicy_tmglobal_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/auditsyslogpolicy_tmglobal_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "auditsyslogpolicy_tmglobal_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"activepolicy":<Integer_value>,

"priority":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditsyslogpolicy_tmglobal_binding/name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"auditsyslogpolicy_tmglobal_binding": [ { "__count": "#no"} ] }
```

auditsyslogpolicy_vpnglobal_binding

Binding object showing the vpnglobal that can be bound to auditsyslogpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the policy. Minimum length = 1
boundto	<String>	Read-write	The entity name to which policy is bound.
activepolicy	<Integer>	Read-only	.
priority	<Integer>	Read-only	.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditsyslogpolicy_vpnglobal_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ auditsyslogpolicy_vpnglobal_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of auditsyslogpolicy_vpnglobal_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/auditsyslogpolicy_vpnglobal_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the auditsyslogpolicy_vpnglobal_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "auditsyslogpolicy_vpnglobal_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"activepolicy":<Integer_value>,

"priority":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditsyslogpolicy_vpnglobal_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/auditsyslogpolicy_vpnglobal_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "auditsyslogpolicy_vpnglobal_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"activepolicy":<Integer_value>,

"priority":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditsyslogpolicy_vpnglobal_binding/name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"auditsyslogpolicy_vpnglobal_binding": [ { "__count": "#no"} ] }
```

auditsyslogpolicy_vpnvserver_binding

Binding object showing the vpnvserver that can be bound to auditsyslogpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
boundto	<String>	Read-write	The entity name to which policy is bound.
name	<String>	Read-write	Name of the policy. Minimum length = 1
activepolicy	<Integer>	Read-only	.
priority	<Integer>	Read-only	.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditsyslogpolicy_vpnvserver_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ auditsyslogpolicy_vpnvserver_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of auditsyslogpolicy_vpnvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/auditsyslogpolicy_vpnvserver_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the auditsyslogpolicy_vpnvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "auditsyslogpolicy_vpnvserver_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"activepolicy":<Integer_value>,

"priority":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditsyslogpolicy_vpnvserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/auditsyslogpolicy_vpnvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "auditsyslogpolicy_vpnvserver_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"activepolicy":<Integer_value>,

"priority":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/auditsyslogpolicy_vpnvserver_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"auditsyslogpolicy_vpnvserver_binding": [ { "__count": "#no"} ] }
```

authentication

Authentication

Authentication configuration.

NAME	DESCRIPTION
authenticationadfsproxyprofile	Configuration for ADFSProxy Profile
authenticationauthnprofile	Configuration for Authentication profile
authenticationazurekeyvault	Configuration for Azure Key Vault entity
authenticationcaptchaaction	Configuration for Captcha Action
authenticationcertaction	Configuration for CERT action

NAME	DESCRIPTION
authenticationcertpolicy	Configuration for CERT policy
authenticationcertpolicy_authenticationvserver_binding	Binding object showing the authenticationvserver that can be bound to authenticationcertpolicy
authenticationcertpolicy_binding	Binding object showing the resources that can be bound to authenticationcertpolicy
authenticationcertpolicy_vpnglobal_binding	Binding object showing the vpnglobal that can be bound to authenticationcertpolicy
authenticationcertpolicy_vpnvserver_binding	Binding object showing the vpnvserver that can be bound to authenticationcertpolicy
authenticationcitrixauthaction	Configuration for Citrix Authentication action
authenticationdfaaction	Configuration for Dfa authentication action
authenticationdfapolicy	Configuration for Dfa authentication policy
authenticationdfapolicy_binding	Binding object showing the resources that can be bound to authenticationdfapolicy
authenticationdfapolicy_vpnvserver_binding	Binding object showing the vpnvserver that can be bound to authenticationdfapolicy
authenticationemailaction	Configuration for Email entity
authenticationepaaction	Configuration for epa action
authenticationldapaction	Configuration for LDAP action
authenticationldappolicy	Configuration for LDAP policy
authenticationldappolicy_authenticationvserver_binding	Binding object showing the authenticationvserver that can be bound to authenticationldappolicy

NAME	DESCRIPTION
authenticationldappolicy_binding	Binding object showing the resources that can be bound to authenticationldappolicy
authenticationldappolicy_systemglobal_binding	Binding object showing the systemglobal that can be bound to authenticationldappolicy
authenticationldappolicy_vpnglobal_binding	Binding object showing the vpnglobal that can be bound to authenticationldappolicy
authenticationldappolicy_vpnvserver_binding	Binding object showing the vpnvserver that can be bound to authenticationldappolicy
authenticationlocalpolicy	Configuration for LOCAL policy
authenticationlocalpolicy_authenticationvserver_binding	Binding object showing the authenticationvserver that can be bound to authenticationlocalpolicy
authenticationlocalpolicy_binding	Binding object showing the resources that can be bound to authenticationlocalpolicy
authenticationlocalpolicy_systemglobal_binding	Binding object showing the systemglobal that can be bound to authenticationlocalpolicy
authenticationlocalpolicy_vpnglobal_binding	Binding object showing the vpnglobal that can be bound to authenticationlocalpolicy
authenticationlocalpolicy_vpnvserver_binding	Binding object showing the vpnvserver that can be bound to authenticationlocalpolicy
authenticationloginschema	
authenticationloginschemapolicy	
authenticationloginschemapolicy_authenticationvserver_binding	
authenticationloginschemapolicy_binding	

NAME	DESCRIPTION
authenticationloginschemapolicy_vpnvserver_binding	
authenticationnegotiateaction	Configuration for Negotiate action
authenticationnegotiatepolicy	Configuration for Negotiate Policy
authenticationnegotiatepolicy_authenticationvserver_binding	Binding object showing the authenticationvserver that can be bound to authenticationnegotiatepolicy
authenticationnegotiatepolicy_binding	Binding object showing the resources that can be bound to authenticationnegotiatepolicy
authenticationnegotiatepolicy_vpnglobal_binding	Binding object showing the vpnglobal that can be bound to authenticationnegotiatepolicy
authenticationnegotiatepolicy_vpnvserver_binding	Binding object showing the vpnvserver that can be bound to authenticationnegotiatepolicy
authenticationnoauthaction	Configuration for no authentication action
authenticationoauthaction	Configuration for OAuth authentication action
authenticationoauthidppolicy	Configuration for AAA OAuth IdentityProvider (IdP) policy
authenticationoauthidppolicy_authenticationvserver_binding	Binding object showing the authenticationvserver that can be bound to authenticationoauthidppolicy
authenticationoauthidppolicy_binding	Binding object showing the resources that can be bound to authenticationoauthidppolicy

NAME	DESCRIPTION
authenticationoauthidppolicy_vpnvserver_binding	Binding object showing the vpnvserver that can be bound to authenticationoauthidppolicy
authenticationoauthidpprofile	Configuration for OAuth Identity Provider (IdP) profile
authenticationpolicy	Configuration for Authentication Policy
authenticationpolicy_authenticationpolicylabel_binding	Binding object showing the authenticationpolicylabel that can be bound to authenticationpolicy
authenticationpolicy_authenticationvserver_binding	Binding object showing the authenticationvserver that can be bound to authenticationpolicy
authenticationpolicy_binding	Binding object showing the resources that can be bound to authenticationpolicy
authenticationpolicy_systemglobal_binding	Binding object showing the systemglobal that can be bound to authenticationpolicy
authenticationpolicylabel	Configuration for authentication policy label
authenticationpolicylabel_authenticationpolicy_binding	Binding object showing the authenticationpolicy that can be bound to authenticationpolicylabel
authenticationpolicylabel_binding	Binding object showing the resources that can be bound to authenticationpolicylabel
authenticationprotecteduseraction	Configuration for Protected user action
authenticationpushservice	Configuration for Service details for sending push notifications
authenticationradiusaction	Configuration for RADIUS action

NAME	DESCRIPTION
authenticationradiuspolicy	Configuration for RADIUS policy
authenticationradiuspolicy_authenticationvserver_binding	Binding object showing the authenticationvserver that can be bound to authenticationradiuspolicy
authenticationradiuspolicy_binding	Binding object showing the resources that can be bound to authenticationradiuspolicy
authenticationradiuspolicy_systemglobal_binding	Binding object showing the systemglobal that can be bound to authenticationradiuspolicy
authenticationradiuspolicy_vpnglobal_binding	Binding object showing the vpnglobal that can be bound to authenticationradiuspolicy
authenticationradiuspolicy_vpnvserver_binding	Binding object showing the vpnvserver that can be bound to authenticationradiuspolicy
authenticationsamlaction	Configuration for AAA Saml action
authenticationsamlidppolicy	Configuration for AAA Saml IdentityProvider (IdP) policy
authenticationsamlidppolicy_authenticationvserver_binding	Binding object showing the authenticationvserver that can be bound to authenticationsamlidppolicy
authenticationsamlidppolicy_binding	Binding object showing the resources that can be bound to authenticationsamlidppolicy
authenticationsamlidppolicy_vpnvserver_binding	Binding object showing the vpnvserver that can be bound to authenticationsamlidppolicy
authenticationsamlidpprofile	Configuration for AAA Saml IdentityProvider (IdP) profile
authenticationsamlpolicy	Configuration for AAA Saml policy

NAME	DESCRIPTION
authenticationsamlpolicy_authenticationvserver_binding	Binding object showing the authenticationvserver that can be bound to authenticationsamlpolicy
authenticationsamlpolicy_binding	Binding object showing the resources that can be bound to authenticationsamlpolicy
authenticationsamlpolicy_vpnglobal_binding	Binding object showing the vpnglobal that can be bound to authenticationsamlpolicy
authenticationsamlpolicy_vpnvserver_binding	Binding object showing the vpnvserver that can be bound to authenticationsamlpolicy
authenticationsmartaccesspolicy	Configuration for SmartAccess policy
authenticationsmartaccesspolicy_authenticationvserver_binding	Binding object showing the authenticationvserver that can be bound to authenticationsmartaccesspolicy
authenticationsmartaccesspolicy_binding	Binding object showing the resources that can be bound to authenticationsmartaccesspolicy
authenticationsmartaccessprofile	Configuration for SmartAccess profile
authenticationstorefrontauthaction	Configuration for Storefront authentication action
authenticationtacacsaction	Configuration for TACACS action
authenticationtacacspolicy	Configuration for TACACS policy
authenticationtacacspolicy_authenticationvserver_binding	Binding object showing the authenticationvserver that can be bound to authenticationtacacspolicy
authenticationtacacspolicy_binding	Binding object showing the resources that can be bound to authenticationtacacspolicy

NAME	DESCRIPTION
authenticationtacacspolicy_systemglobal_binding	Binding object showing the systemglobal that can be bound to authenticationtacacspolicy
authenticationtacacspolicy_vpnglobal_binding	Binding object showing the vpnglobal that can be bound to authenticationtacacspolicy
authenticationtacacspolicy_vpnvserver_binding	Binding object showing the vpnvserver that can be bound to authenticationtacacspolicy
authenticationvserver	Configuration for authentication virtual server
authenticationvserver_auditnslogpolicy_binding	Binding object showing the auditnslogpolicy that can be bound to authenticationvserver
authenticationvserver_auditsyslogpolicy_binding	Binding object showing the auditsyslogpolicy that can be bound to authenticationvserver
authenticationvserver_authenticationcertpolicy_binding	Binding object showing the authenticationcertpolicy that can be bound to authenticationvserver
authenticationvserver_authenticationldappolicy_binding	Binding object showing the authenticationldappolicy that can be bound to authenticationvserver
authenticationvserver_authenticationlocalpolicy_binding	Binding object showing the authenticationlocalpolicy that can be bound to authenticationvserver
authenticationvserver_authenticationloginschemapolicy_binding	Binding object showing the authenticationloginschemapolicy that can be bound to authenticationvserver
authenticationvserver_authenticationnegotiatepolicy_binding	Binding object showing the authenticationnegotiatepolicy that can be bound to authenticationvserver

NAME	DESCRIPTION
authenticationvserver_authenticationoauthidppolicy_binding	Binding object showing the authenticationoauthidppolicy that can be bound to authenticationvserver
authenticationvserver_authenticationpolicy_binding	Binding object showing the authenticationpolicy that can be bound to authenticationvserver
authenticationvserver_authenticationradiuspolicy_binding	Binding object showing the authenticationradiuspolicy that can be bound to authenticationvserver
authenticationvserver_authenticationsamlidppolicy_binding	Binding object showing the authenticationsamlidppolicy that can be bound to authenticationvserver
authenticationvserver_authenticationsamlpolicy_binding	Binding object showing the authenticationsamlpolicy that can be bound to authenticationvserver
authenticationvserver_authenticationsmartaccesspolicy_binding	Binding object showing the authenticationsmartaccesspolicy that can be bound to authenticationvserver
authenticationvserver_authenticationtacacspolicy_binding	Binding object showing the authenticationtacacspolicy that can be bound to authenticationvserver
authenticationvserver_authenticationwebauthpolicy_binding	Binding object showing the authenticationwebauthpolicy that can be bound to authenticationvserver
authenticationvserver_binding	Binding object showing the resources that can be bound to authenticationvserver
authenticationvserver_cachepolicy_binding	Binding object showing the cachepolicy that can be bound to authenticationvserver

NAME	DESCRIPTION
authenticationvserver_cspolicy_binding	Binding object showing the cspolicy that can be bound to authenticationvserver
authenticationvserver_responderpolicy_binding	Binding object showing the responderpolicy that can be bound to authenticationvserver
authenticationvserver_rewritepolicy_binding	Binding object showing the rewritepolicy that can be bound to authenticationvserver
authenticationvserver_tmsessionpolicy_binding	Binding object showing the tmsessionpolicy that can be bound to authenticationvserver
authenticationvserver_vpnportaltheme_binding	Binding object showing the vpnportaltheme that can be bound to authenticationvserver
authenticationwebauthaction	Configuration for Web authentication action
authenticationwebauthpolicy	Configuration for Web authentication policy
authenticationwebauthpolicy_authenticationvserver_binding	Binding object showing the authenticationvserver that can be bound to authenticationwebauthpolicy
authenticationwebauthpolicy_binding	Binding object showing the resources that can be bound to authenticationwebauthpolicy
authenticationwebauthpolicy_systemglobal_binding	Binding object showing the systemglobal that can be bound to authenticationwebauthpolicy
authenticationwebauthpolicy_vpnglobal_binding	Binding object showing the vpnglobal that can be bound to authenticationwebauthpolicy

NAME	DESCRIPTION
authenticationwebauthpolicy_vpnvserver_binding	Binding object showing the vpnvserver that can be bound to authenticationwebauthpolicy

authenticationadfsproxyprofile

Configuration for ADFSProxy Profile resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the adfs proxy profile. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at sign (@), equal sign (=), and hyphen (-) characters. Cannot be changed after the profile is created. CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my push service" or 'my push service'). .

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum length = 1 Maximum length = 127
username	<String>	Read-write	This is the name of an account in directory that would be used to authenticate trust request from ADC acting as a proxy. Minimum length = 1
password	<String>	Read-write	This is the password of an account in directory that would be used to authenticate trust request from ADC acting as a proxy. Minimum length = 1
serverurl	<String>	Read-write	Fully qualified url of the adfs server. Minimum length = 1
certkeyname	<String>	Read-write	SSL certificate of the proxy that is registered at adfs server for trust. Minimum length = 1
adfstruststatus	<String>	Read-only	Describes status of ADFS trust. Default value: INIT Possible values = INIT, FAILED, ESTABLISHED, ESTABLISHED/

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			CONFIGURED, ESTABLISHED_RENEW_SUCCESS, ESTABLISHED_RENEW_FAILED, RENEWED/ CONFIGURED
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationadfsproxyprofile **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationadfsproxyprofile":{

<b>"name":<String_value>,

</b><b>"username":<String_value>,

</b><b>"password":<String_value>,

</b><b>"serverurl":<String_value>,

</b><b>"certkeyname":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationadfsproxyprofile/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationadfsproxyprofile **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationadfsproxyprofile":{

<b>"name":<String_value>,

</b>"username":<String_value>,

"password":<String_value>,

"serverurl":<String_value>,

"certkeyname":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationadfsproxyprofile **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/authenticationadfsproxyprofile? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/authenticationadfsproxyprofile? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of authenticationadfsproxyprofile resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/authenticationadfsproxyprofile? **view=summary**

Use this query-parameter to get the summary output of authenticationadfsproxyprofile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/authenticationadfsproxyprofile? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authenticationadfsproxyprofile resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationadfsproxyprofile": [ {

"name":<String_value>,

"username":<String_value>,

"password":<String_value>,

"serverurl":<String_value>,

"certkeyname":<String_value>,

"adfstruststatus":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationadfsproxyprofile/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/ authenticationadfsproxyprofile/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/authenticationadfsproxyprofile/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of authenticationadfsproxyprofile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationadfsproxyprofile": [ {

"name":<String_value>,

"username":<String_value>,

"password":<String_value>,

"serverurl":<String_value>,

"certkeyname":<String_value>,

"adfstruststatus":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationadfsproxyprofile? **count=yes**
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationadfsproxyprofile": [ { "__count": "#no"} ] }
```

authenticationauthnprofile

Configuration for Authentication profile resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the authentication profile. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after the RADIUS action is added.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum length = 1
authnvsname	<String>	Read-write	Name of the authentication vserver at which authentication should be done. Minimum length = 1 Maximum length = 128
authenticationhost	<String>	Read-write	Hostname of the authentication vserver to which user must be redirected for authentication. Minimum length = 1 Maximum length = 256
authenticationdomain	<String>	Read-write	Domain for which TM cookie must to be set. If unspecified, cookie will be set for FQDN. Minimum length = 1 Maximum length = 256
authenticationlevel	<Integer>	Read-write	Authentication weight or level of the vserver to which this will bound. This is used to order TM vservers based on the protection required. A session that is created by

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			authenticating against TM vserver at given level cannot be used to access TM vserver at a higher level. Minimum value = 0 Maximum value = 255
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationauthnprofile **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationauthnprofile":{

<b>"name":<String_value>,

</b><b>"authnvsname":<String_value>,

</b>"authenticationhost":<String_value>,

"authenticationdomain":<String_value>,

"authenticationlevel":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationauthnprofile/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationauthnprofile **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationauthnprofile":{

<b>"name":<String_value>,

</b>"authnvsname":<String_value>,

"authenticationhost":<String_value>,

"authenticationdomain":<String_value>,

"authenticationlevel":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationauthnprofile? **action=unset**
HTTP Method: POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationauthnprofile":{

<b>"name":<String_value>,

</b>"authenticationdomain":true,

"authenticationlevel":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationauthnprofile **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/authenticationauthnprofile? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/authenticationauthnprofile? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of authenticationauthnprofile resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/authenticationauthnprofile? **view=summary**

Use this query-parameter to get the summary output of authenticationauthnprofile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/authenticationauthnprofile? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authenticationauthnprofile resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationauthnprofile": [ {

"name":<String_value>,

"authnvsname":<String_value>,

"authenticationhost":<String_value>,
```

```
"authenticationdomain":<String_value>,

"authenticationlevel":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationauthnprofile/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/ authenticationauthnprofile/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/authenticationauthnprofile/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of authenticationauthnprofile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationauthnprofile": [ {

"name":<String_value>,

"authnvsname":<String_value>,

"authenticationhost":<String_value>,

"authenticationdomain":<String_value>,

"authenticationlevel":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationauthnprofile? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationauthnprofile": [ { "__count": "#no"} ] }
```

authenticationazurekeyvault

Configuration for Azure Key Vault entity resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the new Azure Key Vault profile. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after an action is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my action" or 'my action'). Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
vaultname	<String>	Read-write	Name of the Azure vault account as configured in azure portal. Minimum length = 1 Maximum length = 63
clientid	<String>	Read-write	Unique identity of the relying party requesting for authentication. Minimum length = 1
clientsecret	<String>	Read-write	Unique secret string to authorize relying party at authorization server. Minimum length = 1
servicekeyname	<String>	Read-write	Friendly name of the Key to be used to compute signature. Minimum length = 1
signaturealg	<String>	Read-write	Algorithm to be used to sign/verify transactions. Default value: RS256 Possible values = RS256
tokenendpoint	<String>	Read-write	URL endpoint on relying party to which the OAuth token is to be sent. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
pushservice	<String>	Read-write	Name of the service used to send push notifications. Minimum length = 1
defaultauthentication group	<String>	Read-write	This is the group that is added to user sessions that match current IdP policy. It can be used in policies to identify relying party trust.
refreshinterval	<Integer>	Read-write	Interval at which access token in obtained. Default value: 50
tenantid	<String>	Read-write	TenantID of the application. This is usually specific to providers such as Microsoft and usually refers to the deployment identifier.
authentication	<String>	Read-write	If authentication is disabled, otp checks are not performed after azure vault keys are obtained. This is useful to distinguish whether user has registered devices. . Default value: ENABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ENABLED, DISABLED
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationazurekeyvault **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationazurekeyvault":{

<b>"name":<String_value>,

</b><b>"vaultname":<String_value>,

</b><b>"clientid":<String_value>,

</b><b>"clientsecret":<String_value>,

</b><b>"servicekeyname":<String_value>,

</b>"signaturealg":<String_value>,

"tokenendpoint":<String_value>,

"pushservice":<String_value>,

"defaultauthenticationgroup":<String_value>,

"refreshinterval":<Integer_value>,
```

```
"tenantid":<String_value>,

"authentication":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationazurekeyvault/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationazurekeyvault **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationazurekeyvault":{

<b>"name":<String_value>,

</b>"vaultname":<String_value>,
```

```
"clientid":<String_value>,

"clientsecret":<String_value>,

"servicekeyname":<String_value>,

"signaturealg":<String_value>,

"tokenendpoint":<String_value>,

"pushservice":<String_value>,

"defaultauthenticationgroup":<String_value>,

"refreshinterval":<Integer_value>,

"tenantid":<String_value>,

"authentication":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationazurekeyvault? **action=unset**
HTTP Method: POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationazurekeyvault":{

<b>"name":<String_value>,

</b>"signaturealg":true,

"pushservice":true,

"defaultauthenticationgroup":true,

"refreshinterval":true,

"authentication":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationazurekeyvault **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/authenticationazurekeyvault? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/authenticationazurekeyvault? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of authenticationazurekeyvault resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/authenticationazurekeyvault? **view=summary**

Use this query-parameter to get the summary output of authenticationazurekeyvault resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/authenticationazurekeyvault? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authenticationazurekeyvault resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationazurekeyvault": [ {

"name":<String_value>,

"vaultname":<String_value>,

"clientid":<String_value>,

"clientsecret":<String_value>,

"servicekeyname":<String_value>,

"signaturealg":<String_value>,

"tokenendpoint":<String_value>,

"pushservice":<String_value>,

"defaultauthenticationgroup":<String_value>,
```

```
"refreshinterval":<Integer_value>,

"tenantid":<String_value>,

"authentication":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationazurekeyvault/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/ authenticationazurekeyvault/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/authenticationazurekeyvault/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of authenticationazurekeyvault resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationazurekeyvault": [ {

"name":<String_value>,

"vaultname":<String_value>,

"clientid":<String_value>,

"clientsecret":<String_value>,

"servicekeyname":<String_value>,

"signaturealg":<String_value>,

"tokenendpoint":<String_value>,

"pushservice":<String_value>,

"defaultauthenticationgroup":<String_value>,

"refreshinterval":<Integer_value>,

"tenantid":<String_value>,

"authentication":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationazurekeyvault? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationazurekeyvault": [ { "__count": "#no"} ] }
```

authenticationcaptchaaction

Configuration for Captcha Action resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the new captcha action. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after an action is created. The following requirement applies

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my action" or 'my action'). Minimum length = 1
serverurl	<String>	Read-write	This is the endpoint at which captcha response is validated.
secretkey	<String>	Read-write	Secret of gateway as established at the captcha source.
sitekey	<String>	Read-write	Sitekey to identify gateway fqdn while loading captcha.
defaultauthentication group	<String>	Read-write	This is the group that is added to user sessions that match current policy.
scorethreshold	<Integer>	Read-write	This is the score threshold value for recaptcha v3. Default value: 5 Minimum value = 0

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum value = 10
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationcaptchaaction **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationcaptchaaction":{

<b>"name":<String_value>,

</b>"serverurl":<String_value>,

<b>"secretkey":<String_value>,

</b><b>"sitekey":<String_value>,

</b>"defaultauthenticationgroup":<String_value>,

"scorethreshold":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationcaptchaaction/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationcaptchaaction **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationcaptchaaction":{

<b>"name":<String_value>,

</b>"serverurl":<String_value>,

"secretkey":<String_value>,

"sitekey":<String_value>,

"defaultauthenticationgroup":<String_value>,

"scorethreshold":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationcaptchaaction? **action=unset**
HTTP Method: POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationcaptchaaction":{

<b>"name":<String_value>,

</b>"serverurl":true,

"defaultauthenticationgroup":true,

"scorethreshold":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationcaptchaaction **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/authenticationcaptchaaction? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/authenticationcaptchaaction? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of authenticationcaptchaaction resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/authenticationcaptchaaction? **view=summary**

Use this query-parameter to get the summary output of authenticationcaptchaaction resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/authenticationcaptchaaction? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authenticationcaptchaaction resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationcaptchaaction": [ {

"name":<String_value>,

"serverurl":<String_value>,

"secretkey":<String_value>,

"sitekey":<String_value>,

"defaultauthenticationgroup":<String_value>,
```

```
"scorethreshold":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationcaptchaaction/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/ authenticationcaptchaaction/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/authenticationcaptchaaction/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of authenticationcaptchaaction resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationcaptchaaction": [ {

"name":<String_value>,

"serverurl":<String_value>,

"secretkey":<String_value>,

"sitekey":<String_value>,

"defaultauthenticationgroup":<String_value>,

"scorethreshold":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationcaptchaaction? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationcaptchaaction": [ { "__count": "#no"} ] }
```

authenticationcertaction

Configuration for CERT action resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the client cert authentication server profile (action). Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after certifcate action is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			"my authentication action" or 'my authentication action'). Minimum length = 1
twofactor	<String>	Read-write	Enables or disables two-factor authentication. Two factor authentication is client cert authentication followed by password authentication. Default value: OFF Possible values = ON, OFF
usernamefield	<String>	Read-write	Client-cert field from which the username is extracted. Must be set to either ""Subject"" and ""Issuer"" (include both sets of double quotation marks). Format: <field>:<subfield>. Minimum length = 1
groupnamefield	<String>	Read-write	Client-cert field from which the group is extracted. Must be set to either

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			""Subject"" and ""Issuer"" (include both sets of double quotation marks). Format: <field>:<subfield>. Minimum length = 1
defaultauthentication group	<String>	Read-write	This is the default group that is chosen when the authentication succeeds in addition to extracted groups.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationcertaction **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationcertaction":{

<b>"name":<String_value>,

</b>"twofactor":<String_value>,

"usernamefield":<String_value>,

"groupnamefield":<String_value>,

"defaultauthenticationgroup":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationcertaction/ name_value<String>
HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationcertaction **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationcertaction":{

<b>"name":<String_value>,

</b>"twofactor":<String_value>,

"usernamefield":<String_value>,

"groupnamefield":<String_value>,

"defaultauthenticationgroup":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationcertaction? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationcertaction":{

<b>"name":<String_value>,

</b>"twofactor":true,

"usernamefield":true,

"groupnamefield":true,

"defaultauthenticationgroup":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationcertaction **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/authenticationcertaction? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/authenticationcertaction? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of authenticationcertaction resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/authenticationcertaction? **view=summary**

Use this query-parameter to get the summary output of authenticationcertaction resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/authenticationcertaction? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authenticationcertaction resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationcertaction": [ {

"name":<String_value>,

"twofactor":<String_value>,
```

```
"usernamefield":<String_value>,

"groupnamefield":<String_value>,

"defaultauthenticationgroup":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationcertaction/ name_value<String>
Query-parameters: attrs http:// <netscaler-ip-address> /nitro/v1/config/authenticationcertaction/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/authenticationcertaction/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of authenticationcertaction resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationcertaction": [ {

"name":<String_value>,

"twofactor":<String_value>,

"usernamefield":<String_value>,

"groupnamefield":<String_value>,

"defaultauthenticationgroup":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationcertaction? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationcertaction": [ { "__count": "#no"} ] }
```

authenticationcertpolicy

Configuration for CERT policy resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the client certificate authentication policy. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after cert authentication policy is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my authentication

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			policy" or 'my authentication policy'). Minimum length = 1
rule	<String>	Read-write	Name of the Citrix ADC named rule, or an expression, that the policy uses to determine whether to attempt to authenticate the user with the authentication server. Minimum length = 1
reqaction	<String>	Read-write	Name of the client cert authentication action to be performed if the policy matches. Minimum length = 1
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET

- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationcertpolicy **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationcertpolicy":{

<b>"name":<String_value>,
```

```
</b><b>"rule":<String_value>,

</b>"reqaction":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationcertpolicy/ name_value<String>
HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationcertpolicy **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationcertpolicy":{

<b>"name":<String_value>,

</b>"rule":<String_value>,

"reqaction":<String_value>
```

```
}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationcertpolicy? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationcertpolicy":{

<b>"name":<String_value>,

</b>"rule":true,

"reqaction":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationcertpolicy **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/authenticationcertpolicy? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/authenticationcertpolicy? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of authenticationcertpolicy resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/authenticationcertpolicy? **view=summary**

Use this query-parameter to get the summary output of authenticationcertpolicy resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/authenticationcertpolicy? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authenticationcertpolicy resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationcertpolicy": [ {

"name":<String_value>,

"rule":<String_value>,

"reqaction":<String_value>,
```

```
"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationcertpolicy/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/authenticationcertpolicy/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/authenticationcertpolicy/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of authenticationcertpolicy resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationcertpolicy": [ {

"name":<String_value>,
```

```
"rule":<String_value>,

"reqaction":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationcertpolicy? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationcertpolicy": [ { "__count": "#no"} ] }
```

authenticationcertpolicy_authenticationvserver_binding

Binding object showing the authenticationvserver that can be bound to authenticationcertpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the client cert authentication policy. Minimum length = 1
boundto	<String>	Read-write	The entity name to which policy is bound.
priority	<Integer>	Read-only	.
activepolicy	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationcertpolicy_authenticationvserver_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ authenticationcertpolicy_authenticationvserver_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of authenticationcertpolicy_authenticationvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ authenticationcertpolicy_authenticationvserver_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authenticationcertpolicy_authenticationvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationcertpolicy_authenticationvserver_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"priority":<Integer_value>,

"activepolicy":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationcertpolicy_authenticationvserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ authenticationcertpolicy_authenticationvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationcertpolicy_authenticationvserver_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"priority":<Integer_value>,

"activepolicy":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationcertpolicy_authenticationvserver_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"authenticationcertpolicy_authenticationvserver_binding": [ { "__count":
"#no"} ] }
```

authenticationcertpolicy_binding

Binding object which returns the resources bound to authenticationcertpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the client cert authentication policy. Minimum length = 1
authenticationcertpolicy_vpnvserver_binding	<authenticationcertpolicy_vpnvserver_binding[]>	Read-only	vpnvserver that can be bound to authenticationcertpolicy.
authenticationcertpolicy_vpnglobal_binding	<authenticationcertpolicy_vpnglobal_binding[]>	Read-only	vpnglobal that can be bound to authenticationcertpolicy.
authenticationcertpolicy_authenticationvserver_binding	<authenticationcertpolicy_authenticationvserver_binding[]>	Read-only	authenticationvserver that can be bound to authenticationcertpolicy.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationcertpolicy_binding/ name_value<String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationcertpolicy_binding": [ {

"name":<String_value>,

"authenticationcertpolicy_authenticationvserver_binding":<authenticationce
rtpolicy_authenticationvserver_binding[]_value>,
```

```
"authenticationcertpolicy_vpnvserver_binding":<authenticationcertpolicy_vpnvserver_binding[]_value>,

"authenticationcertpolicy_vpnglobal_binding":<authenticationcertpolicy_vpnglobal_binding[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationcertpolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/authenticationcertpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationcertpolicy_binding": [ {

"name":<String_value>,

"authenticationcertpolicy_authenticationvserver_binding":<authenticationcertpolicy_authenticationvserver_binding[]_value>,
```

```
"authenticationcertpolicy_vpnvserver_binding":<authenticationcertpolicy_vpnvserver_binding[]_value>,

"authenticationcertpolicy_vpnglobal_binding":<authenticationcertpolicy_vpnglobal_binding[]_value>

}]}
```

authenticationcertpolicy_vpnglobal_binding

Binding object showing the vpnglobal that can be bound to authenticationcertpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the client cert authentication policy. Minimum length = 1
boundto	<String>	Read-write	The entity name to which policy is bound.
priority	<Integer>	Read-only	.
activepolicy	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationcertpolicy_vpnglobal_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ authenticationcertpolicy_vpnglobal_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of authenticationcertpolicy_vpnglobal_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ authenticationcertpolicy_vpnglobal_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authenticationcertpolicy_vpnglobal_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationcertpolicy_vpnglobal_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"priority":<Integer_value>,

"activepolicy":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationcertpolicy_vpnglobal_binding
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/authenticationcertpolicy_vpnglobal_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationcertpolicy_vpnglobal_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"priority":<Integer_value>,

"activepolicy":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationcertpolicy_vpnglobal_binding/name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"authenticationcertpolicy_vpnglobal_binding": [ { "__count": "#no"} ] }
```

authenticationcertpolicy_vpnvserver_binding

Binding object showing the vpnvserver that can be bound to authenticationcertpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the client cert authentication policy. Minimum length = 1
boundto	<String>	Read-write	The entity name to which policy is bound.
activepolicy	<Integer>	Read-only	.
priority	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationcertpolicy_vpnvserver_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ authenticationcertpolicy_vpnvserver_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of authenticationcertpolicy_vpnvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ authenticationcertpolicy_vpnvserver_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authenticationcertpolicy_vpnvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationcertpolicy_vpnvserver_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"activepolicy":<Integer_value>,

"priority":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationcertpolicy_vpnvserver_binding
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/authenticationcertpolicy_vpnvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationcertpolicy_vpnvserver_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"activepolicy":<Integer_value>,

"priority":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationcertpolicy_vpnvserver_binding/name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"authenticationcertpolicy_vpnvserver_binding": [ { "__count": "#no"} ] }
```

authenticationcitrixauthaction

Configuration for Citrix Authentication action resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the new Citrix Authentication action. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after an action is created. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			"my action" or 'my action'). Minimum length = 1
authenticationtype	<String>	Read-write	Type of the Citrix Authentication implementation. Default implementation uses Citrix Cloud Connector. Default value: CITRIXCONNECTOR Possible values = CITRIXCONNECTOR, ATHENA
authentication	<String>	Read-write	Authentication needs to be disabled for searching user object without performing authentication. Default value: ENABLED Possible values = ENABLED, DISABLED
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationcitrixauthaction **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationcitrixauthaction":{

<b>"name":<String_value>,

</b>"authenticationtype":<String_value>,

"authentication":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationcitrixauthaction/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationcitrixauthaction **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationcitrixauthaction":{

<b>"name":<String_value>,

</b>"authenticationtype":<String_value>,

"authentication":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationcitrixauthaction? **action=unset**
HTTP Method: POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationcitrixauthaction":{

<b>"name":<String_value>,

</b>"authenticationtype":true,

"authentication":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationcitrixauthaction **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/authenticationcitrixauthaction? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/authenticationcitrixauthaction? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of authenticationcitrixauthaction resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/authenticationcitrixauthaction? **view=summary**

Use this query-parameter to get the summary output of authenticationcitrixauthaction resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/authenticationcitrixauthaction? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authenticationcitrixauthaction resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationcitrixauthaction": [ {

"name":<String_value>,

"authenticationtype":<String_value>,

"authentication":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationcitrixauthaction/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/ authenticationcitrixauthaction/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/authenticationcitrixauthaction/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of authenticationcitrixauthaction resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationcitrixauthaction": [ {

"name":<String_value>,

"authenticationtype":<String_value>,

"authentication":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationcitrixauthaction? **count=yes**
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationcitrixauthaction": [ { "__count": "#no"} ] }
```

authenticationdfaaction

Configuration for Dfa authentication action resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the DFA action. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after the DFA action is added. Minimum length = 1
clientid	<String>	Read-write	If configured, this string is sent to the DFA server as the X-Citrix-Exchange header value.
serverurl	<String>	Read-write	DFA Server URL.
passphrase	<String>	Read-write	Key shared between the DFA server and the Citrix ADC.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Required to allow the Citrix ADC to communicate with the DFA server. Minimum length = 1
defaultauthenticationgroup	<String>	Read-write	This is the default group that is chosen when the authentication succeeds in addition to extracted groups.
success	<Integer>	Read-only	.
failure	<Integer>	Read-only	.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationdfaaction **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationdfaaction":{

<b>"name":<String_value>,

</b><b>"clientid":<String_value>,

</b><b>"serverurl":<String_value>,

</b><b>"passphrase":<String_value>,

</b>"defaultauthenticationgroup":<String_value>
```

```
}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationdfaaction/ name_value<String>
HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationdfaaction **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationdfaaction":{

<b>"name":<String_value>,

</b>"clientid":<String_value>,

"serverurl":<String_value>,

"passphrase":<String_value>,

"defaultauthenticationgroup":<String_value>
```

```
}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationdfaaction? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationdfaaction":{

<b>"name":<String_value>,

</b>"clientid":true,

"serverurl":true,

"defaultauthenticationgroup":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationdfaaction **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/authenticationdfaaction? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/authenticationdfaaction? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of authenticationdfaaction resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/authenticationdfaaction? **view=summary**

Use this query-parameter to get the summary output of authenticationdfaaction resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/authenticationdfaaction? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authenticationdfaaction resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationdfaaction": [ {

"name":<String_value>,

"passphrase":<String_value>,
```

```
"clientid":<String_value>,

"serverurl":<String_value>,

"success":<Integer_value>,

"failure":<Integer_value>,

"defaultauthenticationgroup":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationdfaaction/ name_value<String>
Query-parameters: attrs http:// <netscaler-ip-address> /nitro/v1/config/authenticationdfaaction/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/authenticationdfaaction/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of authenticationdfaaction resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationdfaaction": [ {

"name":<String_value>,

"passphrase":<String_value>,

"clientid":<String_value>,

"serverurl":<String_value>,

"success":<Integer_value>,

"failure":<Integer_value>,

"defaultauthenticationgroup":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationdfaaction? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationdfaaction": [ { "__count": "#no"} ] }
```

authenticationdfapolicy

Configuration for Dfa authentication policy resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the DFA policy. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after DFA policy is created. The following requirement applies only to the Citrix ADC CLI:

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my authentication policy" or 'my authentication policy'). Minimum length = 1
rule	<String>	Read-write	Name of the Citrix ADC named rule, or an expression, that the policy uses to determine whether to attempt to authenticate the user with the Web server. Minimum length = 1
action	<String>	Read-write	Name of the DFA action to perform if the policy matches. Minimum length = 1
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE

- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationdfapolicy **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationdfapolicy":{

<b>"name":<String_value>,

</b><b>"rule":<String_value>,

</b><b>"action":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationdfapolicy/ name_value<String>
HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationdfapolicy **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationdfapolicy":{

<b>"name":<String_value>,
```

```
</b>"rule":<String_value>,

"action":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationdfapolicy **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/authenticationdfapolicy? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/authenticationdfapolicy? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of authenticationdfapolicy resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/authenticationdfapolicy? **view=summary**

Use this query-parameter to get the summary output of authenticationdfapolicy resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/authenticationdfapolicy? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authenticationdfapolicy resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationdfapolicy": [ {

"name":<String_value>,

"rule":<String_value>,

"action":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationdfapolicy/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/authenticationdfapolicy/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/authenticationdfapolicy/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of authenticationdfapolicy resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationdfapolicy": [ {

"name":<String_value>,

"rule":<String_value>,

"action":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationdfapolicy? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationdfapolicy": [ { "__count": "#no"} ] }
```

authenticationdfapolicy_binding

Binding object which returns the resources bound to authenticationdfapolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the WebAuth policy. Minimum length = 1
authenticationdfapolicy_vpnvserver_binding	<authenticationdfapolicy_vpnvserver_binding[]>	Read-only	vpnvserver that can be bound to authenticationdfapolicy.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationdfapolicy_binding/ name_value<String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationdfapolicy_binding": [ {

"name":<String_value>,
```

```
"authenticationdfapolicy_vpnvserver_binding":<authenticationdfapolicy_vpnv
server_binding[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationdfapolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/authenticationdfapolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationdfapolicy_binding": [ {

"name":<String_value>,

"authenticationdfapolicy_vpnvserver_binding":<authenticationdfapolicy_vpnv
server_binding[]_value>

}]}
```

authenticationdfapolicy_vpnvserver_binding

Binding object showing the vpnvserver that can be bound to authenticationdfapolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
boundto	<String>	Read-write	The entity name to which policy is bound.
name	<String>	Read-write	Name of the WebAuth policy. Minimum length = 1
priority	<Integer>	Read-only	.
activepolicy	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationdfapolicy_vpnvserver_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ authenticationdfapolicy_vpnvserver_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of authenticationdfapolicy_vpnvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ authenticationdfapolicy_vpnvserver_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authenticationdfapolicy_vpnvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationdfapolicy_vpnvserver_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"priority":<Integer_value>,

"activepolicy":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationdfapolicy_vpnvserver_binding
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/authenticationdfapolicy_vpnvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationdfapolicy_vpnvserver_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"priority":<Integer_value>,

"activepolicy":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationdfapolicy_vpnvserver_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"authenticationdfapolicy_vpnvserver_binding": [ { "__count": "#no"} ] }
```

authenticationemailaction

Configuration for Email entity resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the new email action. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after an action is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my action" or 'my action'). Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
username	<String>	Read-write	Username/Clientid/ EmailID to be used to authenticate to the server. Minimum length = 1
password	<String>	Read-write	Password/ Clientsecret to use when authenticating to the server. Minimum length = 1
serverurl	<String>	Read-write	Address of the server that delivers the message. It is fully qualified fqdn such as http(s):// or smtp(s):// for http and smtp protocols respectively. For SMTP, the port number is mandatory like smtps:// smtp.example.com:25. Minimum length = 1
content	<String>	Read-write	Content to be delivered to the user. "$code" string within the content will be replaced with the actual one-time-code to be sent.
defaultauthentication group	<String>	Read-write	This is the group that is added to user sessions that match current IdP policy. It can be used in

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			policies to identify relying party trust.
timeout	<Integer>	Read-write	Time after which the code expires. Default value: 180
type	<String>	Read-write	Type of the email action. Default type is SMTP. Default value: SMTP Possible values = SMTP, ATHENA
emailaddress	<String>	Read-write	An optional expression that yields user's email. When not configured, user's default mail address would be used. When configured, result of this expression is used as destination email address.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE

- UNSET
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationemailaction **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationemailaction":{

<b>"name":<String_value>,

</b><b>"username":<String_value>,

</b><b>"password":<String_value>,

</b><b>"serverurl":<String_value>,

</b>"content":<String_value>,

"defaultauthenticationgroup":<String_value>,

"timeout":<Integer_value>,

"type":<String_value>,

"emailaddress":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationemailaction/ name_value<String>
HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationemailaction **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationemailaction":{

<b>"name":<String_value>,

</b>"username":<String_value>,

"password":<String_value>,

"serverurl":<String_value>,

"content":<String_value>,

"defaultauthenticationgroup":<String_value>,

"timeout":<Integer_value>,

"type":<String_value>,

"emailaddress":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationemailaction? **action=unset** **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationemailaction":{

<b>"name":<String_value>,

</b>"content":true,

"defaultauthenticationgroup":true,

"timeout":true,

"type":true,

"emailaddress":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationemailaction **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/authenticationemailaction? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/authenticationemailaction? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of authenticationemailaction resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/authenticationemailaction? **view=summary**

Use this query-parameter to get the summary output of authenticationemailaction resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/authenticationemailaction? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authenticationemailaction resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationemailaction": [ {

"name":<String_value>,

"username":<String_value>,

"password":<String_value>,

"serverurl":<String_value>,

"content":<String_value>,

"defaultauthenticationgroup":<String_value>,
```

```
"timeout":<Integer_value>,

"type":<String_value>,

"emailaddress":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationemailaction/ name_value<String>
Query-parameters: attrs http:// <netscaler-ip-address> /nitro/v1/config/authenticationemailaction/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/authenticationemailaction/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of authenticationemailaction resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationemailaction": [ {

"name":<String_value>,

"username":<String_value>,

"password":<String_value>,

"serverurl":<String_value>,

"content":<String_value>,

"defaultauthenticationgroup":<String_value>,

"timeout":<Integer_value>,

"type":<String_value>,

"emailaddress":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationemailaction? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationemailaction": [ { "__count": "#no"} ] }
```

authenticationepaaction

Configuration for epa action resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the epa action. Must begin with a letter, number, or the underscore character (_), and must consist only of letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after epa action is created.The following requirement applies only to the Citrix

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			ADC CLI:If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my aaa action" or 'my aaa action'). Minimum length = 1
csecexpr	<String>	Read-write	it holds the ClientSecurityExpression to be sent to the client.
killprocess	<String>	Read-write	String specifying the name of a process to be terminated by the endpoint analysis (EPA) tool. Multiple processes to be delimited by comma.
deletefiles	<String>	Read-write	String specifying the path(s) and name(s) of the files to be deleted by the endpoint analysis (EPA) tool. Multiple files to be delimited by comma.
defaultepagroup	<String>	Read-write	This is the default group that is chosen when the EPA check succeeds. Maximum length = 64

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
quarantinegroup	<String>	Read-write	This is the quarantine group that is chosen when the EPA check fails if configured. Maximum length = 64
deviceposture	<String>	Read-write	Parameter to enable/disable device posture service scan. Possible values = ENABLED, DISABLED
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationepaaction **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationepaaction":{

<b>"name":<String_value>,

</b>"csecexpr":<String_value>,

"killprocess":<String_value>,

"deletefiles":<String_value>,

"defaultepagroup":<String_value>,

"quarantinegroup":<String_value>,
```

```
"deviceposture":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationepaaction/ name_value<String>
HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationepaaction **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationepaaction":{

<b>"name":<String_value>,

</b>"csecexpr":<String_value>,

"killprocess":<String_value>,

"deletefiles":<String_value>,
```

```
"defaultepagroup":<String_value>,

"quarantinegroup":<String_value>,

"deviceposture":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationepaaction? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationepaaction":{

<b>"name":<String_value>,

</b>"killprocess":true,

"deletefiles":true,

"defaultepagroup":true,

"quarantinegroup":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationepaaction **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/authenticationepaaction? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/authenticationepaaction? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of authenticationepaaction resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/authenticationepaaction? **view=summary**

Use this query-parameter to get the summary output of authenticationepaaction resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/authenticationepaaction? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authenticationepaaction resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationepaaction": [ {

"name":<String_value>,

"killprocess":<String_value>,

"deletefiles":<String_value>,

"defaultepagroup":<String_value>,

"quarantinegroup":<String_value>,

"csecexpr":<String_value>,

"deviceposture":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationepaaction/ name_value<String>
Query-parameters: attrs http:// <netscaler-ip-address> /nitro/v1/config/authenticationepaaction/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/authenticationepaaction/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of authenticationepaaction resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationepaaction": [ {

"name":<String_value>,

"killprocess":<String_value>,

"deletefiles":<String_value>,

"defaultepagroup":<String_value>,

"quarantinegroup":<String_value>,

"csecexpr":<String_value>,

"deviceposture":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationepaaction? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationepaaction": [ { "__count": "#no"} ] }
```

authenticationldapaction

Configuration for LDAP action resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the new LDAP action. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after the LDAP action is added.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my authentication action" or 'my authentication action'). Minimum length = 1
serverip	<String>	Read-write	IP address assigned to the LDAP server. Minimum length = 1
servername	<String>	Read-write	LDAP server name as a FQDN. Mutually exclusive with LDAP IP address. Minimum length = 1
serverport	<Integer>	Read-write	Port on which the LDAP server accepts connections. Default value: 389 Minimum value = 1
authtimeout	<Integer>	Read-write	Number of seconds the Citrix ADC waits for a response from the RADIUS server.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: 3 Minimum value = 1
ldapbase	<String>	Read-write	Base (node) from which to start LDAP searches. If the LDAP server is running locally, the default value of base is dc=netscaler, dc=com.
ldapbinddn	<String>	Read-write	Full distinguished name (DN) that is used to bind to the LDAP server. Default: cn=Manager,dc=netscaler,dc=com.
ldapbinddnpassword	<String>	Read-write	Password used to bind to the LDAP server. Minimum length = 1
ldaploginname	<String>	Read-write	LDAP login name attribute. The Citrix ADC uses the LDAP login name to query external LDAP servers or Active Directories.
searchfilter	<String>	Read-write	String to be combined with the default LDAP user

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			search string to form the search value. For example, if the search filter "vpnallowed=true" is combined with the LDAP login name "samaccount" and the user-supplied username is "bob", the result is the LDAP search string ""(vpnallowed=true)(samaccount=bob)"" (Be sure to enclose the search string in two sets of double quotation marks; both sets are needed.). Minimum length = 1
groupattrname	<String>	Read-write	LDAP group attribute name. Used for group extraction on the LDAP server.
subattributename	<String>	Read-write	LDAP group sub-attribute name. Used for group extraction from the LDAP server.
sectype	<String>	Read-write	Type of security used for communications between the Citrix ADC and the LDAP server. For the PLAINTEXT setting,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			no encryption is required. Default value: PLAINTEXT Possible values = PLAINTEXT, TLS, SSL
svrtype	<String>	Read-write	The type of LDAP server. Default value: AAA_LDAP_SERVER_TYPE_DEFAULT Possible values = AD, NDS
ssonameattribute	<String>	Read-write	LDAP single signon (SSO) attribute. The Citrix ADC uses the SSO name attribute to query external LDAP servers or Active Directories for an alternate username.
authentication	<String>	Read-write	Perform LDAP authentication. If authentication is disabled, any LDAP authentication attempt returns authentication

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			success if the user is found. CAUTION! Authentication should be disabled only for authorization group extraction or where other (non-LDAP) authentication methods are in use and either bound to a primary list or flagged as secondary. Default value: ENABLED Possible values = ENABLED, DISABLED
requireuser	<String>	Read-write	Require a successful user search for authentication. CAUTION! This field should be set to NO only if usersearch not required [Both username validation as well as password validation skipped] and (non-LDAP) authentication methods are in use

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			and either bound to a primary list or flagged as secondary. Default value: YES Possible values = YES, NO
passwdchange	<String>	Read-write	Allow password change requests. Default value: DISABLED Possible values = ENABLED, DISABLED
nestedgroupextraction	<String>	Read-write	Allow nested group extraction, in which the Citrix ADC queries external LDAP servers to determine whether a group is part of another group. Default value: OFF Possible values = ON, OFF
maxnestinglevel	<Integer>	Read-write	If nested group extraction is ON, specifies the number of levels up to which group extraction is performed. Default value: 2

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum value = 2
followreferrals	<String>	Read-write	Setting this option to ON enables following LDAP referrals received from the LDAP server. Default value: OFF Possible values = ON, OFF
maxldapreferrals	<Integer>	Read-write	Specifies the maximum number of nested referrals to follow. Default value: 1 Minimum value = 1
referraldnslookup	<String>	Read-write	Specifies the DNS Record lookup Type for the referrals. Default value: A-REC Possible values = A-REC, SRV-REC, MSSRV-REC
mssrvrecordlocation	<String>	Read-write	MSSRV Specific parameter. Used to locate the DNS node to which the SRV record pertains in the domainname. The domainname is appended to it to form the srv record.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Example : For "dc._msdcs", the srv record formed is _ldap._tcp.dc._msdcs.<domainname>.
validateservercert	<String>	Read-write	When to validate LDAP server certs. Default value: NO Possible values = YES, NO
ldaphostname	<String>	Read-write	Hostname for the LDAP server. If -validateServerCert is ON then this must be the host name on the certificate from the LDAP server. A hostname mismatch will cause a connection failure.
groupnameidentifier	<String>	Read-write	Name that uniquely identifies a group in LDAP or Active Directory.
groupsearchattribute	<String>	Read-write	LDAP group search attribute. Used to determine to which groups a group belongs.
groupsearchsubattribute	<String>	Read-write	LDAP group search subattribute.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Used to determine to which groups a group belongs.
groupsearchfilter	<String>	Read-write	String to be combined with the default LDAP group search string to form the search value. For example, the group search filter ""vpnallowed=true"" when combined with the group identifier ""samaccount"" and the group name ""g1"" yields the LDAP search string ""(;(vpnallowed=true)(samaccount=g1)"". If nestedGroupExtraction is ENABLED, the filter is applied on the first level group search as well, otherwise first level groups (of which user is a direct member of) will be fetched without applying this filter. (Be sure to enclose the search string in two sets of double quotation marks; both sets are needed.).

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
defaultauthentication group	<String>	Read-write	This is the default group that is chosen when the authentication succeeds in addition to extracted groups.
attribute1	<String>	Read-write	Expression that would be evaluated to extract attribute1 from the ldap response.
attribute2	<String>	Read-write	Expression that would be evaluated to extract attribute2 from the ldap response.
attribute3	<String>	Read-write	Expression that would be evaluated to extract attribute3 from the ldap response.
attribute4	<String>	Read-write	Expression that would be evaluated to extract attribute4 from the ldap response.
attribute5	<String>	Read-write	Expression that would be evaluated to extract attribute5 from the ldap response.
attribute6	<String>	Read-write	Expression that would be evaluated to extract attribute6

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			from the ldap response.
attribute7	<String>	Read-write	Expression that would be evaluated to extract attribute7 from the ldap response.
attribute8	<String>	Read-write	Expression that would be evaluated to extract attribute8 from the ldap response.
attribute9	<String>	Read-write	Expression that would be evaluated to extract attribute9 from the ldap response.
attribute10	<String>	Read-write	Expression that would be evaluated to extract attribute10 from the ldap response.
attribute11	<String>	Read-write	Expression that would be evaluated to extract attribute11 from the ldap response.
attribute12	<String>	Read-write	Expression that would be evaluated to extract attribute12 from the ldap response.
attribute13	<String>	Read-write	Expression that would be evaluated to extract attribute13

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			from the ldap response.
attribute14	<String>	Read-write	Expression that would be evaluated to extract attribute14 from the ldap response.
attribute15	<String>	Read-write	Expression that would be evaluated to extract attribute15 from the ldap response.
attribute16	<String>	Read-write	Expression that would be evaluated to extract attribute16 from the ldap response.
attributes	<String>	Read-write	List of attribute names separated by ',' which needs to be fetched from ldap server. Note that preceeding and trailing spaces will be removed. Attribute name can be 127 bytes and total length of this string should not cross 2047 bytes. These attributes have multi-value support separated

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			by ',' and stored as key-value pair in AAA session.
sshpublickey	<String>	Read-write	SSH PublicKey is attribute on AD. This attribute is used to retrieve ssh PublicKey for RBA authentication. Minimum length = 1
pushservice	<String>	Read-write	Name of the service used to send push notifications. Minimum length = 1
otpsecret	<String>	Read-write	OneTimePassword(OTP) Secret key attribute on AD. This attribute is used to store and retrieve secret key used for OTP check. Minimum length = 1
email	<String>	Read-write	The Citrix ADC uses the email attribute to query the Active Directory for the email id of a user. Default value: mail Maximum length = 128
kbattribute	<String>	Read-write	KnowledgeBasedAuthentication(KBA) attribute on AD. This attribute is used to store and retrieve

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			preconfigured Question and Answer knowledge base used for KBA authentication. Minimum length = 1 Maximum length = 127
alternateemailattr	<String>	Read-write	The NetScaler appliance uses the alternateive email attribute to query the Active Directory for the alternative email id of a user. Maximum length = 128
cloudattributes	<String>	Read-write	The Citrix ADC uses the cloud attributes to extract additional attributes from LDAP servers required for Citrix Cloud operations. Default value: DISABLED Possible values = ENABLED, DISABLED
passwordlessmgmtaccess	<String>	Read-write	This feature configures NetScaler management access to use LDAP exclusively for retrieving user group information. It

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			ensures that LDAP is not used for authenticating user logins (i.e., verifying passwords) for NetScaler management access. Default value: DISABLED Possible values = ENABLED, DISABLED
success	<Integer>	Read-only	.
failure	<Integer>	Read-only	.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationldapaction **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationldapaction":{

<b>"name":<String_value>,

</b>"serverip":<String_value>,

"servername":<String_value>,
```

```
"serverport":<Integer_value>,

"authtimeout":<Integer_value>,

"ldapbase":<String_value>,

"ldapbinddn":<String_value>,

"ldapbinddnpassword":<String_value>,

"ldaploginname":<String_value>,

"searchfilter":<String_value>,

"groupattrname":<String_value>,

"subattributename":<String_value>,

"sectype":<String_value>,

"svrtype":<String_value>,

"ssonameattribute":<String_value>,

"authentication":<String_value>,

"requireuser":<String_value>,

"passwdchange":<String_value>,

"nestedgroupextraction":<String_value>,

"maxnestinglevel":<Integer_value>,

"followreferrals":<String_value>,

"maxldapreferrals":<Integer_value>,

"referraldnslookup":<String_value>,

"mssrvrecordlocation":<String_value>,

"validateservercert":<String_value>,
```

```
"ldaphostname":<String_value>,

"groupnameidentifier":<String_value>,

"groupsearchattribute":<String_value>,

"groupsearchsubattribute":<String_value>,

"groupsearchfilter":<String_value>,

"defaultauthenticationgroup":<String_value>,

"attribute1":<String_value>,

"attribute2":<String_value>,

"attribute3":<String_value>,

"attribute4":<String_value>,

"attribute5":<String_value>,

"attribute6":<String_value>,

"attribute7":<String_value>,

"attribute8":<String_value>,

"attribute9":<String_value>,

"attribute10":<String_value>,

"attribute11":<String_value>,

"attribute12":<String_value>,

"attribute13":<String_value>,

"attribute14":<String_value>,

"attribute15":<String_value>,

"attribute16":<String_value>,
```

```
"attributes":<String_value>,

"sshpublickey":<String_value>,

"pushservice":<String_value>,

"otpsecret":<String_value>,

"email":<String_value>,

"kbattribute":<String_value>,

"alternateemailattr":<String_value>,

"cloudattributes":<String_value>,

"passwordlessmgmtaccess":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationldapaction/ name_value<String>
HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationldapaction **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationldapaction":{

<b>"name":<String_value>,

</b>"serverip":<String_value>,

"servername":<String_value>,

"serverport":<Integer_value>,

"authtimeout":<Integer_value>,

"ldapbase":<String_value>,

"ldapbinddn":<String_value>,

"ldapbinddnpassword":<String_value>,

"ldaploginname":<String_value>,

"searchfilter":<String_value>,

"groupattrname":<String_value>,

"subattributename":<String_value>,

"sectype":<String_value>,

"svrtype":<String_value>,

"ssonameattribute":<String_value>,

"authentication":<String_value>,

"requireuser":<String_value>,

"passwdchange":<String_value>,
```

```
"validateservercert":<String_value>,

"ldaphostname":<String_value>,

"nestedgroupextraction":<String_value>,

"maxnestinglevel":<Integer_value>,

"groupnameidentifier":<String_value>,

"groupsearchattribute":<String_value>,

"groupsearchsubattribute":<String_value>,

"groupsearchfilter":<String_value>,

"followreferrals":<String_value>,

"maxldapreferrals":<Integer_value>,

"referraldnslookup":<String_value>,

"mssrvrecordlocation":<String_value>,

"defaultauthenticationgroup":<String_value>,

"attribute1":<String_value>,

"attribute2":<String_value>,

"attribute3":<String_value>,

"attribute4":<String_value>,

"attribute5":<String_value>,

"attribute6":<String_value>,

"attribute7":<String_value>,

"attribute8":<String_value>,

"attribute9":<String_value>,
```

```
"attribute10":<String_value>,

"attribute11":<String_value>,

"attribute12":<String_value>,

"attribute13":<String_value>,

"attribute14":<String_value>,

"attribute15":<String_value>,

"attribute16":<String_value>,

"attributes":<String_value>,

"otpsecret":<String_value>,

"sshpublickey":<String_value>,

"pushservice":<String_value>,

"email":<String_value>,

"kbattribute":<String_value>,

"alternateemailattr":<String_value>,

"cloudattributes":<String_value>,

"passwordlessmgmtaccess":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationldapaction? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationldapaction":{

<b>"name":<String_value>,

</b>"serverport":true,

"authtimeout":true,

"ldapbase":true,

"ldapbinddn":true,

"ldapbinddnpassword":true,

"ldaploginname":true,

"searchfilter":true,

"groupattrname":true,

"subattributename":true,

"sectype":true,

"svrtype":true,

"ssonameattribute":true,

"authentication":true,

"requireuser":true,
```

```
"passwdchange":true,

"validateservercert":true,

"ldaphostname":true,

"nestedgroupextraction":true,

"maxnestinglevel":true,

"groupnameidentifier":true,

"groupsearchattribute":true,

"groupsearchsubattribute":true,

"groupsearchfilter":true,

"followreferrals":true,

"maxldapreferrals":true,

"referraldnslookup":true,

"mssrvrecordlocation":true,

"defaultauthenticationgroup":true,

"attribute1":true,

"attribute2":true,

"attribute3":true,

"attribute4":true,

"attribute5":true,

"attribute6":true,

"attribute7":true,

"attribute8":true,
```

```
"attribute9":true,

"attribute10":true,

"attribute11":true,

"attribute12":true,

"attribute13":true,

"attribute14":true,

"attribute15":true,

"attribute16":true,

"attributes":true,

"otpsecret":true,

"pushservice":true,

"email":true,

"kbattribute":true,

"alternateemailattr":true,

"cloudattributes":true,

"passwordlessmgmtaccess":true

}}
```


Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationldapaction **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/authenticationldapaction? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/authenticationldapaction? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of authenticationldapaction resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/authenticationldapaction? **view=summary**

Use this query-parameter to get the summary output of authenticationldapaction resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/authenticationldapaction? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authenticationldapaction resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationldapaction": [ {

"name":<String_value>,

"serverip":<String_value>,

"servername":<String_value>,

"serverport":<Integer_value>,

"authtimeout":<Integer_value>,

"ldapbinddn":<String_value>,

"ldapbinddnpassword":<String_value>,

"ldaploginname":<String_value>,

"ldapbase":<String_value>,

"searchfilter":<String_value>,

"groupattrname":<String_value>,

"subattributename":<String_value>,

"sectype":<String_value>,

"svrtype":<String_value>,

"ssonameattribute":<String_value>,

"authentication":<String_value>,

"requireuser":<String_value>,

"success":<Integer_value>,

"failure":<Integer_value>,

"nestedgroupextraction":<String_value>,

"maxnestinglevel":<Integer_value>,
```

```
"followreferrals":<String_value>,

"maxldapreferrals":<Integer_value>,

"referraldnslookup":<String_value>,

"mssrvrecordlocation":<String_value>,

"validateservercert":<String_value>,

"ldaphostname":<String_value>,

"groupnameidentifier":<String_value>,

"groupsearchattribute":<String_value>,

"groupsearchsubattribute":<String_value>,

"groupsearchfilter":<String_value>,

"passwdchange":<String_value>,

"defaultauthenticationgroup":<String_value>,

"attribute1":<String_value>,

"attribute2":<String_value>,

"attribute3":<String_value>,

"attribute4":<String_value>,

"attribute5":<String_value>,

"attribute6":<String_value>,

"attribute7":<String_value>,

"attribute8":<String_value>,

"attribute9":<String_value>,

"attribute10":<String_value>,
```

```
"attribute11":<String_value>,

"attribute12":<String_value>,

"attribute13":<String_value>,

"attribute14":<String_value>,

"attribute15":<String_value>,

"attribute16":<String_value>,

"attributes":<String_value>,

"otpsecret":<String_value>,

"sshpublickey":<String_value>,

"pushservice":<String_value>,

"email":<String_value>,

"kbattribute":<String_value>,

"alternateemailattr":<String_value>,

"cloudattributes":<String_value>,

"passwordlessmgmtaccess":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationldapaction/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/authenticationldapaction/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/authenticationldapaction/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of authenticationldapaction resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationldapaction": [ {

"name":<String_value>,

"serverip":<String_value>,

"servername":<String_value>,

"serverport":<Integer_value>,

"authtimeout":<Integer_value>,

"ldapbinddn":<String_value>,

"ldapbinddnpassword":<String_value>,

"ldaploginname":<String_value>,
```

```
"ldapbase":<String_value>,

"searchfilter":<String_value>,

"groupattrname":<String_value>,

"subattributename":<String_value>,

"sectype":<String_value>,

"svrtype":<String_value>,

"ssonameattribute":<String_value>,

"authentication":<String_value>,

"requireuser":<String_value>,

"success":<Integer_value>,

"failure":<Integer_value>,

"nestedgroupextraction":<String_value>,

"maxnestinglevel":<Integer_value>,

"followreferrals":<String_value>,

"maxldapreferrals":<Integer_value>,

"referraldnslookup":<String_value>,

"mssrvrecordlocation":<String_value>,

"validateservercert":<String_value>,

"ldaphostname":<String_value>,

"groupnameidentifier":<String_value>,

"groupsearchattribute":<String_value>,

"groupsearchsubattribute":<String_value>,
```

```
"groupsearchfilter":<String_value>,

"passwdchange":<String_value>,

"defaultauthenticationgroup":<String_value>,

"attribute1":<String_value>,

"attribute2":<String_value>,

"attribute3":<String_value>,

"attribute4":<String_value>,

"attribute5":<String_value>,

"attribute6":<String_value>,

"attribute7":<String_value>,

"attribute8":<String_value>,

"attribute9":<String_value>,

"attribute10":<String_value>,

"attribute11":<String_value>,

"attribute12":<String_value>,

"attribute13":<String_value>,

"attribute14":<String_value>,

"attribute15":<String_value>,

"attribute16":<String_value>,

"attributes":<String_value>,

"otpsecret":<String_value>,

"sshpublickey":<String_value>,
```

```
"pushservice":<String_value>,

"email":<String_value>,

"kbattribute":<String_value>,

"alternateemailattr":<String_value>,

"cloudattributes":<String_value>,

"passwordlessmgmtaccess":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationldapaction? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationldapaction": [ { "__count": "#no"} ] }
```

authenticationldappolicy

Configuration for LDAP policy resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the LDAP policy. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after LDAP policy is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my authentication policy" or 'my

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			authentication policy'). Minimum length = 1
rule	<String>	Read-write	Name of the Citrix ADC named rule, or an expression, that the policy uses to determine whether to attempt to authenticate the user with the LDAP server. Minimum length = 1
reqaction	<String>	Read-write	Name of the LDAP action to perform if the policy matches. Minimum length = 1
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationldappolicy **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationldappolicy":{

<b>"name":<String_value>,

</b><b>"rule":<String_value>,

</b>"reqaction":<String_value>
```

```
}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationldappolicy/ name_value<String>
HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationldappolicy **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationldappolicy":{

<b>"name":<String_value>,

</b>"rule":<String_value>,

"reqaction":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationldappolicy? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationldappolicy":{

<b>"name":<String_value>,

</b>"rule":true,

"reqaction":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationldappolicy **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/authenticationldappolicy? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/authenticationldappolicy? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of authenticationldappolicy resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/authenticationldappolicy? **view=summary**

Use this query-parameter to get the summary output of authenticationldappolicy resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/authenticationldappolicy? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authenticationldappolicy resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationldappolicy": [ {

"name":<String_value>,

"rule":<String_value>,

"reqaction":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationldappolicy/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/authenticationldappolicy/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/authenticationldappolicy/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of authenticationldappolicy resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationldappolicy": [ {

"name":<String_value>,

"rule":<String_value>,

"reqaction":<String_value>,
```

```
"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationldappolicy? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationldappolicy": [ { "__count": "#no"} ] }
```

authenticationldappolicy_authenticationvserver_binding

Binding object showing the authenticationvserver that can be bound to authenticationldappolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
boundto	<String>	Read-write	The entity name to which policy is bound.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the LDAP policy. Minimum length = 1
activepolicy	<Integer>	Read-only	.
priority	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationldappolicy_authenticationvserver_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ authenticationldappolicy_authenticationvserver_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of authenticationldappolicy_authenticationvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ authenticationldappolicy_authenticationvserver_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authenticationldappolicy_authenticationvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationldappolicy_authenticationvserver_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"activepolicy":<Integer_value>,

"priority":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationldappolicy_authenticationvserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ authenticationldappolicy_authenticationvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationldappolicy_authenticationvserver_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"activepolicy":<Integer_value>,

"priority":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationldappolicy_authenticationvserver_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"authenticationldappolicy_authenticationvserver_binding": [ { "__count":
"#no"} ] }
```

authenticationldappolicy_binding

Binding object which returns the resources bound to authenticationldappolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the LDAP policy. Minimum length = 1
authenticationldappolicy_systemglobal_binding	<authenticationldappolicy_systemglobal_binding[]>	Read-only	systemglobal that can be bound to authenticationldappolicy.
authenticationldappolicy_vpnglobal_binding	<authenticationldappolicy_vpnglobal_binding[]>	Read-only	vpnglobal that can be bound to authenticationldappolicy.
authenticationldappolicy_vpnvserver_binding	<authenticationldappolicy_vpnvserver_binding[]>	Read-only	vpnvserver that can be bound to authenticationldappolicy.
authenticationldappolicy_authenticationvserver_binding	<authenticationldappolicy_authenticationvserver_binding[]>	Read-only	authenticationvserver that can be bound to authenticationldappolicy.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationldappolicy_binding/name_value<String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationldappolicy_binding": [ {

"name":<String_value>,

"authenticationldappolicy_authenticationvserver_binding":<authenticationld
appolicy_authenticationvserver_binding[]_value>,

"authenticationldappolicy_vpnglobal_binding":<authenticationldappolicy_vpn
global_binding[]_value>,

"authenticationldappolicy_systemglobal_binding":<authenticationldappolicy_
systemglobal_binding[]_value>,

"authenticationldappolicy_vpnvserver_binding":<authenticationldappolicy_vp
nvserver_binding[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationldappolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/authenticationldappolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationldappolicy_binding": [ {

"name":<String_value>,

"authenticationldappolicy_authenticationvserver_binding":<authenticationldappolicy_authenticationvserver_binding[]_value>,

"authenticationldappolicy_vpnglobal_binding":<authenticationldappolicy_vpnglobal_binding[]_value>,

"authenticationldappolicy_systemglobal_binding":<authenticationldappolicy_systemglobal_binding[]_value>,

"authenticationldappolicy_vpnvserver_binding":<authenticationldappolicy_vpnvserver_binding[]_value>

}]}
```

authenticationldappolicy_systemglobal_binding

Binding object showing the systemglobal that can be bound to authenticationldappolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the LDAP policy. Minimum length = 1
boundto	<String>	Read-write	The entity name to which policy is bound.
priority	<Integer>	Read-only	.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
activepolicy	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationldappolicy_systemglobal_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/authenticationldappolicy_systemglobal_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of authenticationldappolicy_systemglobal_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ authenticationldappolicy_systemglobal_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authenticationldappolicy_systemglobal_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationldappolicy_systemglobal_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"priority":<Integer_value>,
```

```
"activepolicy":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationldappolicy_systemglobal_binding
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/authenticationldappolicy_systemglobal_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationldappolicy_systemglobal_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"priority":<Integer_value>,

"activepolicy":<Integer_value>
```

```
}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationldappolicy_systemglobal_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"authenticationldappolicy_systemglobal_binding": [ { "__count":
"#no"} ] }
```

authenticationldappolicy_vpnglobal_binding

Binding object showing the vpnglobal that can be bound to authenticationldappolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
boundto	<String>	Read-write	The entity name to which policy is bound.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the LDAP policy. Minimum length = 1
priority	<Integer>	Read-only	.
activepolicy	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationldappolicy_vpnglobal_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ authenticationldappolicy_vpnglobal_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of authenticationldappolicy_vpnglobal_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ authenticationldappolicy_vpnglobal_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authenticationldappolicy_vpnglobal_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationldappolicy_vpnglobal_binding": [ {

"boundto":<String_value>,
```

```
"name":<String_value>,

"priority":<Integer_value>,

"activepolicy":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationldappolicy_vpnglobal_binding
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/authenticationldappolicy_vpnglobal_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationldappolicy_vpnglobal_binding": [ {

"boundto":<String_value>,

"name":<String_value>,
```

```
"priority":<Integer_value>,

"activepolicy":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationldappolicy_vpnglobal_binding/name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"authenticationldappolicy_vpnglobal_binding": [ { "__count": "#no"} ] }
```

authenticationldappolicy_vpnvserver_binding

Binding object showing the vpnvserver that can be bound to authenticationldappolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
boundto	<String>	Read-write	The entity name to which policy is bound.
name	<String>	Read-write	Name of the LDAP policy. Minimum length = 1
priority	<Integer>	Read-only	.
activepolicy	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationldappolicy_vpnvserver_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ authenticationldappolicy_vpnvserver_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of authenticationldappolicy_vpnvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ authenticationldappolicy_vpnvserver_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authenticationldappolicy_vpnvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationldappolicy_vpnvserver_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"priority":<Integer_value>,

"activepolicy":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationldappolicy_vpnvserver_binding
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/authenticationldappolicy_vpnvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationldappolicy_vpnvserver_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"priority":<Integer_value>,

"activepolicy":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationldappolicy_vpnvserver_binding/name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"authenticationldappolicy_vpnvserver_binding": [ { "__count": "#no"} ] }
```

authenticationlocalpolicy

Configuration for LOCAL policy resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the local authentication policy. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after local policy is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my authentication policy" or 'my authentication policy').
rule	<String>	Read-write	Name of the Citrix ADC named rule, or an expression, that

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			the policy uses to perform the authentication.
reqaction	<String>	Read-only	The name of the RADIUS action the policy uses.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.
- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationlocalpolicy **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationlocalpolicy":{

<b>"name":<String_value>,

</b><b>"rule":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationlocalpolicy/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationlocalpolicy **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationlocalpolicy":{

<b>"name":<String_value>,

</b>"rule":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationlocalpolicy **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/authenticationlocalpolicy? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/authenticationlocalpolicy? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of authenticationlocalpolicy resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/authenticationlocalpolicy? **view=summary**

Use this query-parameter to get the summary output of authenticationlocalpolicy resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/authenticationlocalpolicy? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authenticationlocalpolicy resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationlocalpolicy": [ {

"name":<String_value>,

"rule":<String_value>,

"reqaction":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

```
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationlocalpolicy/ name_value<String>
Query-parameters: attrs http:// <netscaler-ip-address> /nitro/v1/config/authenticationlocalpolicy/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/authenticationlocalpolicy/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of authenticationlocalpolicy resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationlocalpolicy": [ {

"name":<String_value>,

"rule":<String_value>,

"reqaction":<String_value>,
```

```
"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationlocalpolicy? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationlocalpolicy": [ { "__count": "#no"} ] }
```

authenticationlocalpolicy_authenticationvserver_binding

Binding object showing the authenticationvserver that can be bound to authenticationlocalpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
boundto	<String>	Read-write	The entity name to which policy is bound.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the local authentication policy.
activepolicy	<Integer>	Read-only	.
priority	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationlocalpolicy_authenticationvserver_binding/ name_value<String>

Query-parameters:

filter

http:// <netscaler-ip-address> /nitro/v1/config/ authenticationlocalpolicy_authenticationvserver_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of authenticationlocalpolicy_authenticationvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination

http:// <netscaler-ip-address> /nitro/v1/config/ authenticationlocalpolicy_authenticationvserver_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authenticationlocalpolicy_authenticationvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationlocalpolicy_authenticationvserver_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"activepolicy":<Integer_value>,

"priority":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationlocalpolicy_authenticationvserver_binding

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters:

bulkbindings

http:// <netscaler-ip-address> /nitro/v1/config/ authenticationlocalpolicy_authenticationvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationlocalpolicy_authenticationvserver_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"activepolicy":<Integer_value>,

"priority":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationlocalpolicy_authenticationvserver_binding/ name_value<String> ? **count=yes**

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"authenticationlocalpolicy_authenticationvserver_binding": [ { "__count":
"#no"} ] }
```

authenticationlocalpolicy_binding

Binding object which returns the resources bound to authenticationlocalpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the local authentication policy.
authenticationlocalpolicy_systemglobal_binding	<authenticationlocalpolicy_systemglobal_binding[]>	Read-only	systemglobal that can be bound to authenticationlocalpolicy.
authenticationlocalpolicy_vpnvserver_binding	<authenticationlocalpolicy_vpnvserver_binding[]>	Read-only	vpnvserver that can be bound to authenticationlocalpolicy.
authenticationlocalpolicy_vpnglobal_binding	<authenticationlocalpolicy_vpnglobal_binding[]>	Read-only	vpnglobal that can be bound to authenticationlocalpolicy.
authenticationlocalpolicy_authenticationvserver_binding	<authenticationlocalpolicy_authenticationvserver_binding[]>	Read-only	authenticationvserver that can be bound to

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			authenticationlocalpolicy.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.
- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationlocalpolicy_binding/name_value<String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationlocalpolicy_binding": [ {

"name":<String_value>,

"authenticationlocalpolicy_systemglobal_binding":<authenticationlocalpolic
y_systemglobal_binding[]_value>,

"authenticationlocalpolicy_vpnglobal_binding":<authenticationlocalpolicy_v
pnglobal_binding[]_value>,

"authenticationlocalpolicy_authenticationvserver_binding":<authenticationl
ocalpolicy_authenticationvserver_binding[]_value>,

"authenticationlocalpolicy_vpnvserver_binding":<authenticationlocalpolicy_
vpnvserver_binding[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationlocalpolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ authenticationlocalpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationlocalpolicy_binding": [ {

"name":<String_value>,

"authenticationlocalpolicy_systemglobal_binding":<authenticationlocalpolic
y_systemglobal_binding[]_value>,

"authenticationlocalpolicy_vpnglobal_binding":<authenticationlocalpolicy_v
pnglobal_binding[]_value>,

"authenticationlocalpolicy_authenticationvserver_binding":<authenticationl
ocalpolicy_authenticationvserver_binding[]_value>,

"authenticationlocalpolicy_vpnvserver_binding":<authenticationlocalpolicy_
vpnvserver_binding[]_value>

}]}
```

authenticationlocalpolicy_systemglobal_binding

Binding object showing the systemglobal that can be bound to authenticationlocalpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the local authentication policy.
boundto	<String>	Read-write	The entity name to which policy is bound.
priority	<Integer>	Read-only	.
activepolicy	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.
- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationlocalpolicy_systemglobal_binding/ name_value<String>

Query-parameters:

filter

http:// <netscaler-ip-address> /nitro/v1/config/authenticationlocalpolicy_systemglobal_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of authenticationlocalpolicy_systemglobal_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination

http:// <netscaler-ip-address> /nitro/v1/config/authenticationlocalpolicy_systemglobal_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authenticationlocalpolicy_systemglobal_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationlocalpolicy_systemglobal_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"priority":<Integer_value>,

"activepolicy":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationlocalpolicy_systemglobal_binding

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters:

bulkbindings

http:// <netscaler-ip-address> /nitro/v1/config/authenticationlocalpolicy_systemglobal_binding?**bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationlocalpolicy_systemglobal_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"priority":<Integer_value>,

"activepolicy":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationlocalpolicy_systemglobal_binding/ name_value<String> ? **count=yes**

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"authenticationlocalpolicy_systemglobal_binding": [ { "__count":
"#no"} ] }
```

authenticationlocalpolicy_vpnglobal_binding

Binding object showing the vpnglobal that can be bound to authenticationlocalpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
boundto	<String>	Read-write	The entity name to which policy is bound.
name	<String>	Read-write	Name of the local authentication policy.
priority	<Integer>	Read-only	.
activepolicy	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationlocalpolicy_vpnglobal_binding/name_value<String>

Query-parameters:

filter

http:// <netscaler-ip-address> /nitro/v1/config/authenticationlocalpolicy_vpnglobal_binding/name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of authenticationlocalpolicy_vpnglobal_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination

http:// <netscaler-ip-address> /nitro/v1/config/authenticationlocalpolicy_vpnglobal_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authenticationlocalpolicy_vpnglobal_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationlocalpolicy_vpnglobal_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"priority":<Integer_value>,

"activepolicy":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationlocalpolicy_vpnglobal_binding

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters:

bulkbindings

http:// <netscaler-ip-address> /nitro/v1/config/authenticationlocalpolicy_vpnglobal_binding?**bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationlocalpolicy_vpnglobal_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"priority":<Integer_value>,
```

```
"activepolicy":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationlocalpolicy_vpnglobal_binding/name_value<String> ? **count=yes**

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"authenticationlocalpolicy_vpnglobal_binding": [ { "__count": "#no"} ] }
```

authenticationlocalpolicy_vpnvserver_binding

Binding object showing the vpnvserver that can be bound to authenticationlocalpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the local authentication policy.
boundto	<String>	Read-write	The entity name to which policy is bound.
activepolicy	<Integer>	Read-only	.
priority	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationlocalpolicy_vpnvserver_binding/name_value<String>

Query-parameters:

filter

http:// <netscaler-ip-address> /nitro/v1/config/authenticationlocalpolicy_vpnvserver_binding/name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of authenticationlocalpolicy_vpnvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination

http:// <netscaler-ip-address> /nitro/v1/config/authenticationlocalpolicy_vpnvserver_binding/name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authenticationlocalpolicy_vpnvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationlocalpolicy_vpnvserver_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"activepolicy":<Integer_value>,

"priority":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationlocalpolicy_vpnvserver_binding

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters:

bulkbindings

http:// <netscaler-ip-address> /nitro/v1/config/authenticationlocalpolicy_vpnvserver_binding?**bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationlocalpolicy_vpnvserver_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"activepolicy":<Integer_value>,

"priority":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationlocalpolicy_vpnvserver_binding/name_value<String> ? **count=yes**

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"authenticationlocalpolicy_vpnvserver_binding": [ { "__count": "#no"} ] }
```

authenticationloginschema

Configuration for 0 resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the new login schema. Login schema defines the way login form is rendered. It provides a way to customize the fields that are shown to the user. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after an action is created.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my action" or 'my action'). Minimum length = 1
authenticationschema	<String>	Read-write	Name of the file for reading authentication schema to be sent for Login Page UI. This file should contain xml definition of elements as per Citrix Forms Authentication Protocol to be able to render login form. If administrator does not want to prompt users for additional credentials but continue with previously obtained credentials, then "noschema" can be given as argument. Please note that this applies only to loginSchemas that

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			are used with user-defined factors, and not the vserver factor. Minimum length = 1
userexpression	<String>	Read-write	Expression for username extraction during login. This can be any relevant advanced policy expression. Minimum length = 1
passwdexpression	<String>	Read-write	Expression for password extraction during login. This can be any relevant advanced policy expression. Minimum length = 1
usercredentialindex	<Integer>	Read-write	The index at which user entered username should be stored in session. Minimum value = 1 Maximum value = 16
passwordcredentialindex	<Integer>	Read-write	The index at which user entered password should be stored in session. Minimum value = 1 Maximum value = 16

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
authenticationstrength	<Integer>	Read-write	Weight of the current authentication. Minimum value = 0 Maximum value = 65535
ssocredentials	<String>	Read-write	This option indicates whether current factor credentials are the default SSO (SingleSignOn) credentials. Default value: NO Possible values = YES, NO
builtin	<String[]>	Read-only	Indicates that a variable is a built-in (SYSTEM INTERNAL) type. Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL
feature	<String>	Read-only	The feature to be checked while applying this config.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD

- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationloginschema **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationloginschema":{

<b>"name":<String_value>,

</b><b>"authenticationschema":<String_value>,

</b>"userexpression":<String_value>,

"passwdexpression":<String_value>,

"usercredentialindex":<Integer_value>,

"passwordcredentialindex":<Integer_value>,

"authenticationstrength":<Integer_value>,

"ssocredentials":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationloginschema/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationloginschema **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationloginschema":{

<b>"name":<String_value>,

</b>"authenticationschema":<String_value>,

"userexpression":<String_value>,

"passwdexpression":<String_value>,

"usercredentialindex":<Integer_value>,

"passwordcredentialindex":<Integer_value>,

"authenticationstrength":<Integer_value>,

"ssocredentials":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationloginschema? **action=unset**
HTTP Method: POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationloginschema":{

<b>"name":<String_value>,

</b>"userexpression":true,

"passwdexpression":true,

"usercredentialindex":true,

"passwordcredentialindex":true,

"authenticationstrength":true,

"ssocredentials":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationloginschema **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/authenticationloginschema? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/authenticationloginschema? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of authenticationloginschema resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/authenticationloginschema? **view=summary**

Use this query-parameter to get the summary output of authenticationloginschema resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/authenticationloginschema? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authenticationloginschema resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationloginschema": [ {

"name":<String_value>,

"authenticationschema":<String_value>,

"userexpression":<String_value>,
```

```
"passwdexpression":<String_value>,

"usercredentialindex":<Integer_value>,

"passwordcredentialindex":<Integer_value>,

"authenticationstrength":<Integer_value>,

"ssocredentials":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationloginschema/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/ authenticationloginschema/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/authenticationloginschema/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of authenticationloginschema resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationloginschema": [ {

"name":<String_value>,

"authenticationschema":<String_value>,

"userexpression":<String_value>,

"passwdexpression":<String_value>,

"usercredentialindex":<Integer_value>,

"passwordcredentialindex":<Integer_value>,

"authenticationstrength":<Integer_value>,

"ssocredentials":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationloginschema? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationloginschema": [ { "__count": "#no"} ] }
```

authenticationloginschemapolicy

Configuration for 0 resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the LoginSchema policy. This is used for selecting parameters for user logon. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			be changed after the policy is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my policy" or 'my policy'). Minimum length = 1
rule	<String>	Read-write	Expression which is evaluated to choose a profile for authentication. The following requirements apply only to the Citrix ADC CLI: * If the expression includes one or more spaces, enclose the entire expression in double quotation marks. * If the expression itself includes double quotation

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			marks, escape the quotations by using the \ character. * Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks. Minimum length = 1
action	<String>	Read-write	Name of the profile to apply to requests or connections that match this policy. * NOOP - Do not take any specific action when this policy evaluates to true. This is useful to implicitly go to a different policy set. * RESET - Reset the client connection by closing it. The client program, such as a browser, will handle this and may inform the user. The client may then resend

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			the request if desired. * DROP - Drop the request without sending a response to the user. Minimum length = 1
undefaction	<String>	Read-write	Action to perform if the result of policy evaluation is undefined (UNDEF). An UNDEF event indicates an internal error condition. Only the above built-in actions can be used.
comment	<String>	Read-write	Any comments to preserve information about this policy.
logaction	<String>	Read-write	Name of messagelog action to use when a request matches this policy.
newname	<String>	Read-write	New name for the LoginSchema policy. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space ( ), at (@),

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			equals (=), colon (:), and underscore characters. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my loginschemapolicy policy" or 'my loginschemapolicy policy'). Minimum length = 1
hits	<Integer>	Read-only	Number of hits.
undefhits	<Integer>	Read-only	Number of Undef hits.
builtin	<String[]>	Read-only	Flag to determine if policy is built-in or not. Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
feature	<String>	Read-only	The feature to be checked while applying this config.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT
- RENAME

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationloginschemapolicy **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationloginschemapolicy":{

<b>"name":<String_value>,

</b><b>"rule":<String_value>,

</b><b>"action":<String_value>,

</b>"undefaction":<String_value>,

"comment":<String_value>,

"logaction":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationloginschemapolicy/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationloginschemapolicy **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationloginschemapolicy":{

<b>"name":<String_value>,

</b>"rule":<String_value>,

"action":<String_value>,

"undefaction":<String_value>,

"comment":<String_value>,

"logaction":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationloginschemapolicy?**action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationloginschemapolicy":{

<b>"name":<String_value>,

</b>"undefaction":true,

"comment":true,

"logaction":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

RENAME

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationloginschemapolicy?**action=rename HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationloginschemapolicy":{

<b>"name":<String_value>,

</b><b>"newname":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationloginschemapolicy **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/authenticationloginschemapolicy?**attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/authenticationloginschemapolicy?**filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of authenticationloginschemapolicy resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/authenticationloginschemapolicy?**view=summary**

Use this query-parameter to get the summary output of authenticationloginschemapolicy resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/authenticationloginschemapolicy?**pagesize=#no;pageno=#no**

Use this query-parameter to get the authenticationloginschemapolicy resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationloginschemapolicy": [ {

"name":<String_value>,

"rule":<String_value>,

"action":<String_value>,

"undefaction":<String_value>,

"comment":<String_value>,

"logaction":<String_value>,

"hits":<Integer_value>,

"undefhits":<Integer_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationloginschemapolicy/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/ authenticationloginschemapolicy/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/authenticationloginschemapolicy/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of authenticationloginschemapolicy resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationloginschemapolicy": [ {

"name":<String_value>,

"rule":<String_value>,

"action":<String_value>,

"undefaction":<String_value>,
```

```
"comment":<String_value>,

"logaction":<String_value>,

"hits":<Integer_value>,

"undefhits":<Integer_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationloginschemapolicy? **count=yes**
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationloginschemapolicy": [ { "__count": "#no"} ] }
```

authenticationloginschemapolicy_authenticationvserver_binding

Binding object showing the authenticationvserver that can be bound to authenticationloginschemapolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the LoginSchema policy for which to display detailed information. Minimum length = 1
boundto	<String>	Read-write	The entity name to which policy is bound.
labelname	<String>	Read-only	Name of the label to invoke if the current policy rule evaluates to TRUE.
gotopriorityexpression	<String>	Read-only	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
activepolicy	<Integer>	Read-only	.
labeltype	<String>	Read-only	Type of policy label invocation. Possible values = reqvserver, resvserver, policylabel

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
priority	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationloginschemapolicy_authenticationvserver_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ authenticationloginschemapolicy_authenticationvserver_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of authenticationloginschemapolicy_authenticationvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ authenticationloginschemapolicy_authenticationvserver_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authenticationloginschemapolicy_authenticationvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationloginschemapolicy_authenticationvserver_binding": [ {

"name":<String_value>,

"boundto":<String_value>,
```

```
"labelname":<String_value>,

"gotopriorityexpression":<String_value>,

"activepolicy":<Integer_value>,

"labeltype":<String_value>,

"priority":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationloginschemapolicy_authenticationvserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ authenticationloginschemapolicy_authenticationvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationloginschemapolicy_authenticationvserver_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"labelname":<String_value>,

"gotopriorityexpression":<String_value>,

"activepolicy":<Integer_value>,

"labeltype":<String_value>,

"priority":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationloginschemapolicy_authenticationvserver_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"authenticationloginschemapolicy_authenticationvserver_binding":
[ { "__count": "#no"} ] }
```

authenticationloginschemapolicy_binding

Binding object which returns the resources bound to authenticationloginschemapolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the LoginSchema policy for which to display detailed information. Minimum length = 1
authenticationloginschemapolicy_authenticationvserver_binding	<authenticationloginschemapolicy_authenticationvserver_binding[]>	Read-only	authenticationvserver that can be bound to authenticationloginschemapolicy.
authenticationloginschemapolicy_vpnvserver_binding	<authenticationloginschemapolicy_vpnvserver_binding[]>	Read-only	vpnvserver that can be bound to authenticationloginschemapolicy.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationloginschemapolicy_binding/name_value<String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationloginschemapolicy_binding": [ {

"name":<String_value>,

"authenticationloginschemapolicy_vpnvserver_binding":<authenticationlogins
chemapolicy_vpnvserver_binding[]_value>,

"authenticationloginschemapolicy_authenticationvserver_binding":<authentic
ationloginschemapolicy_authenticationvserver_binding[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationloginschemapolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/authenticationloginschemapolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationloginschemapolicy_binding": [ {

"name":<String_value>,

"authenticationloginschemapolicy_vpnvserver_binding":<authenticationlogins
chemapolicy_vpnvserver_binding[]_value>,

"authenticationloginschemapolicy_authenticationvserver_binding":<authentic
ationloginschemapolicy_authenticationvserver_binding[]_value>

}]}
```

authenticationloginschemapolicy_vpnvserver_binding

Binding object showing the vpnvserver that can be bound to authenticationloginschemapolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the LoginSchema policy for which to display detailed information. Minimum length = 1
boundto	<String>	Read-write	The entity name to which policy is bound.
priority	<Integer>	Read-only	.
labeltype	<String>	Read-only	Type of policy label invocation. Possible values = reqvserver, resvserver, policylabel

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
activepolicy	<Integer>	Read-only	.
gotopriorityexpression	<String>	Read-only	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
labelname	<String>	Read-only	Name of the label to invoke if the current policy rule evaluates to TRUE.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationloginschemapolicy_vpnvserver_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ authenticationloginschemapolicy_vpnvserver_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of authenticationloginschemapolicy_vpnvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ authenticationloginschemapolicy_vpnvserver_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authenticationloginschemapolicy_vpnvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationloginschemapolicy_vpnvserver_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"priority":<Integer_value>,

"labeltype":<String_value>,

"activepolicy":<Integer_value>,

"gotopriorityexpression":<String_value>,

"labelname":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationloginschemapolicy_vpnvserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ authenticationloginschemapolicy_vpnvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationloginschemapolicy_vpnvserver_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"priority":<Integer_value>,

"labeltype":<String_value>,

"activepolicy":<Integer_value>,

"gotopriorityexpression":<String_value>,

"labelname":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationloginschemapolicy_vpnvserver_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"authenticationloginschemapolicy_vpnvserver_binding": [ { "__count":
"#no"} ] }
```

authenticationnegotiateaction

Configuration for Negotiate action resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the AD KDC server profile (negotiate action). Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after AD KDC server profile is created.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my authentication action" or 'my authentication action'). Minimum length = 1
domain	<String>	Read-write	Domain name of the service principal that represnts Citrix ADC. Minimum length = 1
domainuser	<String>	Read-write	User name of the account that is mapped with Citrix ADC principal. This can be given along with domain and password when keytab file is not available. If username is given along with keytab file, then that keytab file will be searched for this user's credentials. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
domainuserpasswd	<String>	Read-write	Password of the account that is mapped to the Citrix ADC principal. Minimum length = 1
ou	<String>	Read-write	Active Directory organizational units (OU) attribute. Minimum length = 1
defaultauthentication group	<String>	Read-write	This is the default group that is chosen when the authentication succeeds in addition to extracted groups.
keytab	<String>	Read-write	The path to the keytab file that is used to decrypt kerberos tickets presented to Citrix ADC. If keytab is not available, domain/ username/password can be specified in the negotiate action configuration. Minimum length = 1
ntlmpath	<String>	Read-write	The path to the site that is enabled for NTLM authentication, including FQDN of the server. This is used when clients fallback to NTLM. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
kcdspn	<String>	Read-only	Host SPN extracted from keytab file.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationnegotiateaction **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationnegotiateaction":{

<b>"name":<String_value>,

</b>"domain":<String_value>,

"domainuser":<String_value>,

"domainuserpasswd":<String_value>,

"ou":<String_value>,

"defaultauthenticationgroup":<String_value>,

"keytab":<String_value>,

"ntlmpath":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationnegotiateaction/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationnegotiateaction **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationnegotiateaction":{

<b>"name":<String_value>,

</b>"domain":<String_value>,

"domainuser":<String_value>,

"domainuserpasswd":<String_value>,

"ou":<String_value>,

"defaultauthenticationgroup":<String_value>,

"keytab":<String_value>,
```

```
"ntlmpath":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationnegotiateaction? **action=unset**
HTTP Method: POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationnegotiateaction":{

<b>"name":<String_value>,

</b>"domain":true,

"domainuser":true,

"domainuserpasswd":true,

"ou":true,

"defaultauthenticationgroup":true,

"ntlmpath":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationnegotiateaction **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/authenticationnegotiateaction? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/authenticationnegotiateaction? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of authenticationnegotiateaction resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/authenticationnegotiateaction? **view=summary**

Use this query-parameter to get the summary output of authenticationnegotiateaction resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/authenticationnegotiateaction? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authenticationnegotiateaction resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationnegotiateaction": [ {

"name":<String_value>,

"domain":<String_value>,

"domainuser":<String_value>,

"domainuserpasswd":<String_value>,

"ou":<String_value>,

"defaultauthenticationgroup":<String_value>,

"keytab":<String_value>,

"kcdspn":<String_value>,

"ntlmpath":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationnegotiateaction/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/ authenticationnegotiateaction/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/authenticationnegotiateaction/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of authenticationnegotiateaction resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationnegotiateaction": [ {

"name":<String_value>,

"domain":<String_value>,

"domainuser":<String_value>,

"domainuserpasswd":<String_value>,

"ou":<String_value>,

"defaultauthenticationgroup":<String_value>,

"keytab":<String_value>,

"kcdspn":<String_value>,

"ntlmpath":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationnegotiateaction? **count=yes**
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationnegotiateaction": [ { "__count": "#no"} ] }
```

authenticationnegotiatepolicy

Configuration for Negotiate Policy resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the negotiate authentication policy. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after AD KCD (negotiate) policy is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my authentication policy" or 'my authentication policy'). Minimum length = 1
rule	<String>	Read-write	Name of the Citrix ADC named rule, or an expression, that the policy uses to determine whether to attempt to authenticate the user with the AD KCD server. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
reqaction	<String>	Read-write	Name of the negotiate action to perform if the policy matches. Minimum length = 1
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationnegotiatepolicy **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationnegotiatepolicy":{

<b>"name":<String_value>,

</b><b>"rule":<String_value>,

</b><b>"reqaction":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationnegotiatepolicy/name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationnegotiatepolicy **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationnegotiatepolicy":{

<b>"name":<String_value>,

</b>"rule":<String_value>,

"reqaction":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationnegotiatepolicy **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/authenticationnegotiatepolicy?**attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/authenticationnegotiatepolicy? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of authenticationnegotiatepolicy resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/authenticationnegotiatepolicy? **view=summary**

Use this query-parameter to get the summary output of authenticationnegotiatepolicy resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/authenticationnegotiatepolicy? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authenticationnegotiatepolicy resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationnegotiatepolicy": [ {

"name":<String_value>,

"rule":<String_value>,

"reqaction":<String_value>,
```

```
"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationnegotiatepolicy/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/ authenticationnegotiatepolicy/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/authenticationnegotiatepolicy/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of authenticationnegotiatepolicy resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationnegotiatepolicy": [ {

"name":<String_value>,
```

```
"rule":<String_value>,

"reqaction":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationnegotiatepolicy? **count=yes**
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationnegotiatepolicy": [ { "__count": "#no"} ] }
```

authenticationnegotiatepolicy_authenticationvserver_binding

Binding object showing the authenticationvserver that can be bound to authenticationnegotiatepolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
boundto	<String>	Read-write	The entity name to which policy is bound.
name	<String>	Read-write	Name of the negotiate policy. Minimum length = 1
activepolicy	<Integer>	Read-only	.
priority	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationnegotiatepolicy_authenticationvserver_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ authenticationnegotiatepolicy_authenticationvserver_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of authenticationnegotiatepolicy_authenticationvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ authenticationnegotiatepolicy_authenticationvserver_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authenticationnegotiatepolicy_authenticationvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationnegotiatepolicy_authenticationvserver_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"activepolicy":<Integer_value>,

"priority":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationnegotiatepolicy_authenticationvserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ authenticationnegotiatepolicy_authenticationvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationnegotiatepolicy_authenticationvserver_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"activepolicy":<Integer_value>,

"priority":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationnegotiatepolicy_authenticationvserver_binding/ name_value<String> ? **count=yes**
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"authenticationnegotiatepolicy_authenticationvserver_binding":
[ { "__count": "#no"} ] }
```

authenticationnegotiatepolicy_binding

Binding object which returns the resources bound to authenticationnegotiatepolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the negotiate policy. Minimum length = 1
authenticationnegotiatepolicy_authenticationvserver_binding	<authenticationnegotiatepolicy_authenticationvserver_binding[]>	Read-only	authenticationvserver that can be bound to authenticationnegotiatepolicy.
authenticationnegotiatepolicy_vpnvserver_binding	<authenticationnegotiatepolicy_vpnvserver_binding[]>	Read-only	vpnvserver that can be bound to authenticationnegotiatepolicy.
authenticationnegotiatepolicy_vpnglobal_binding	<authenticationnegotiatepolicy_vpnglobal_binding[]>	Read-only	vpnglobal that can be bound to authenticationnegotiatepolicy.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationnegotiatepolicy_binding/name_value<String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationnegotiatepolicy_binding": [ {

"name":<String_value>,

"authenticationnegotiatepolicy_vpnvserver_binding":<authenticationnegotiatepolicy_vpnvserver_binding[]_value>,
```

```
"authenticationnegotiatepolicy_vpnglobal_binding":<authenticationnegotiate
policy_vpnglobal_binding[]_value>,

"authenticationnegotiatepolicy_authenticationvserver_binding":<authenticat
ionnegotiatepolicy_authenticationvserver_binding[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationnegotiatepolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/authenticationnegotiatepolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationnegotiatepolicy_binding": [ {

"name":<String_value>,

"authenticationnegotiatepolicy_vpnvserver_binding":<authenticationnegotiat
epolicy_vpnvserver_binding[]_value>,
```

```
"authenticationnegotiatepolicy_vpnglobal_binding":<authenticationnegotiate
policy_vpnglobal_binding[]_value>,

"authenticationnegotiatepolicy_authenticationvserver_binding":<authenticat
ionnegotiatepolicy_authenticationvserver_binding[]_value>

}]}
```

authenticationnegotiatepolicy_vpnglobal_binding

Binding object showing the vpnglobal that can be bound to authenticationnegotiatepolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
boundto	<String>	Read-write	The entity name to which policy is bound.
name	<String>	Read-write	Name of the negotiate policy. Minimum length = 1
activepolicy	<Integer>	Read-only	.
priority	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationnegotiatepolicy_vpnglobal_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/authenticationnegotiatepolicy_vpnglobal_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of authenticationnegotiatepolicy_vpnglobal_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/authenticationnegotiatepolicy_vpnglobal_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authenticationnegotiatepolicy_vpnglobal_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationnegotiatepolicy_vpnglobal_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"activepolicy":<Integer_value>,

"priority":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationnegotiatepolicy_vpnglobal_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ authenticationnegotiatepolicy_vpnglobal_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationnegotiatepolicy_vpnglobal_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"activepolicy":<Integer_value>,

"priority":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationnegotiatepolicy_vpnglobal_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"authenticationnegotiatepolicy_vpnglobal_binding": [ { "__count":
"#no"} ] }
```

authenticationnegotiatepolicy_vpnvserver_binding

Binding object showing the vpnvserver that can be bound to authenticationnegotiatepolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the negotiate policy. Minimum length = 1
boundto	<String>	Read-write	The entity name to which policy is bound.
activepolicy	<Integer>	Read-only	.
priority	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationnegotiatepolicy_vpnvserver_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/authenticationnegotiatepolicy_vpnvserver_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of authenticationnegotiatepolicy_vpnvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/authenticationnegotiatepolicy_vpnvserver_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authenticationnegotiatepolicy_vpnvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationnegotiatepolicy_vpnvserver_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"activepolicy":<Integer_value>,

"priority":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationnegotiatepolicy_vpnvserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ authenticationnegotiatepolicy_vpnvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationnegotiatepolicy_vpnvserver_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"activepolicy":<Integer_value>,

"priority":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationnegotiatepolicy_vpnvserver_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"authenticationnegotiatepolicy_vpnvserver_binding": [ { "__count":
"#no"} ] }
```

authenticationnoauthaction

Configuration for no authentication action resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the new no-authentication action. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after an action is created. The following requirement applies

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my action" or 'my action'). Minimum length = 1
defaultauthenticationgroup	<String>	Read-write	This is the group that is added to user sessions that match current policy.
builtin	<String[]>	Read-only	Indicates that a variable is a built-in (SYSTEM INTERNAL) type. Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL
feature	<String>	Read-only	The feature to be checked while applying this config.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationnoauthaction **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationnoauthaction":{

<b>"name":<String_value>,

</b>"defaultauthenticationgroup":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationnoauthaction/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationnoauthaction **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationnoauthaction":{

<b>"name":<String_value>,

</b>"defaultauthenticationgroup":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationnoauthaction? **action=unset**
HTTP Method: POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationnoauthaction":{

<b>"name":<String_value>,

</b>"defaultauthenticationgroup":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationnoauthaction **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/authenticationnoauthaction? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/authenticationnoauthaction? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of authenticationnoauthaction resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/authenticationnoauthaction? **view=summary**

Use this query-parameter to get the summary output of authenticationnoauthaction resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/authenticationnoauthaction? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authenticationnoauthaction resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationnoauthaction": [ {

"name":<String_value>,

"defaultauthenticationgroup":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationnoauthaction/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/ authenticationnoauthaction/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/authenticationnoauthaction/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of authenticationnoauthaction resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationnoauthaction": [ {

"name":<String_value>,

"defaultauthenticationgroup":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationnoauthaction? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationnoauthaction": [ { "__count": "#no"} ] }
```

authenticationoauthaction

Configuration for OAuth authentication action resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the OAuth Authentication action. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after the profile is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			name in double or single quotation marks (for example, "my authentication action" or 'my authentication action'). Minimum length = 1
oauthtype	<String>	Read-write	Type of the OAuth implementation. Default value is generic implementation that is applicable for most deployments. Default value: GENERIC Possible values = GENERIC, INTUNE
authorizationendpoint	<String>	Read-write	Authorization endpoint/url to which unauthenticated user will be redirected. Citrix ADC redirects user to this endpoint by adding query parameters including clientid. If this parameter not specified then as default value we take Token Endpoint/URL value. Please note that Authorization Endpoint or Token Endpoint is

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			mandatory for oauthAction.
tokenendpoint	<String>	Read-write	URL to which OAuth token will be posted to verify its authenticity. User obtains this token from Authorization server upon successful authentication. Citrix ADC will validate presented token by posting it to the URL configured.
idtokendecryptendpoint	<String>	Read-write	URL to which obtained idtoken will be posted to get a decrypted user identity. Encrypted idtoken will be obtained by posting OAuth token to token endpoint. In order to decrypt idtoken, Citrix ADC posts request to the URL configured.
clientid	<String>	Read-write	Unique identity of the client/user who is getting authenticated. Authorization server infers client configuration using this ID. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
clientsecret	<String>	Read-write	Secret string established by user and authorization server. Minimum length = 1
defaultauthentication group	<String>	Read-write	This is the default group that is chosen when the authentication succeeds in addition to extracted groups.
oauthmiscflags	<String[]>	Read-write	Option to set/unset miscellaneous feature flags. Available values function as follows: * Base64Encode_Authorization_With_Padding - On setting this value, for endpoints (token and introspect), basic authorization header will be base64 encoded with padding. * EnableJWTRequest - By enabling this field, Authorisation request to IDP will

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			have jwt signed 'request' parameter. Possible values = Base64Encode_Authorization_With_Padding, EnableJWTRequest
attribute1	<String>	Read-write	Name of the attribute to be extracted from OAuth Token and to be stored in the attribute1.
attribute2	<String>	Read-write	Name of the attribute to be extracted from OAuth Token and to be stored in the attribute2.
attribute3	<String>	Read-write	Name of the attribute to be extracted from OAuth Token and to be stored in the attribute3.
attribute4	<String>	Read-write	Name of the attribute to be extracted from OAuth Token and to be stored in the attribute4.
attribute5	<String>	Read-write	Name of the attribute to be extracted from OAuth Token and to be stored in the attribute5.
attribute6	<String>	Read-write	Name of the attribute to be extracted from

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			OAuth Token and to be stored in the attribute6.
attribute7	<String>	Read-write	Name of the attribute to be extracted from OAuth Token and to be stored in the attribute7.
attribute8	<String>	Read-write	Name of the attribute to be extracted from OAuth Token and to be stored in the attribute8.
attribute9	<String>	Read-write	Name of the attribute to be extracted from OAuth Token and to be stored in the attribute9.
attribute10	<String>	Read-write	Name of the attribute to be extracted from OAuth Token and to be stored in the attribute10.
attribute11	<String>	Read-write	Name of the attribute to be extracted from OAuth Token and to be stored in the attribute11.
attribute12	<String>	Read-write	Name of the attribute to be extracted from OAuth Token and to be stored in the attribute12.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
attribute13	<String>	Read-write	Name of the attribute to be extracted from OAuth Token and to be stored in the attribute13.
attribute14	<String>	Read-write	Name of the attribute to be extracted from OAuth Token and to be stored in the attribute14.
attribute15	<String>	Read-write	Name of the attribute to be extracted from OAuth Token and to be stored in the attribute15.
attribute16	<String>	Read-write	Name of the attribute to be extracted from OAuth Token and to be stored in the attribute16.
attributes	<String>	Read-write	List of attribute names separated by ',' which needs to be extracted. Note that preceding and trailing spaces will be removed. Attribute name can be 127 bytes and total length of this string should not cross 1023 bytes. These attributes have multi-value

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			support separated by ',' and stored as key-value pair in AAA session.
tenantid	<String>	Read-write	TenantID of the application. This is usually specific to providers such as Microsoft and usually refers to the deployment identifier.
graphendpoint	<String>	Read-write	URL of the Graph API service to learn Enterprise Mobility Services (EMS) endpoints.
refreshinterval	<Integer>	Read-write	Interval at which services are monitored for necessary configuration. Default value: 1440
certendpoint	<String>	Read-write	URL of the endpoint that contains JWKs (Json Web Key) for JWT (Json Web Token) verification.
audience	<String>	Read-write	Audience for which token sent by Authorization server is applicable. This is typically entity name or url that represents the recipient.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
usernamefield	<String>	Read-write	Attribute in the token from which username should be extracted. Minimum length = 1
skewtime	<Integer>	Read-write	This option specifies the allowed clock skew in number of minutes that Citrix ADC allows on an incoming token. For example, if skewTime is 10, then token would be valid from (current time - 10) min to (current time + 10) min, ie 20min in all. Default value: 5
issuer	<String>	Read-write	Identity of the server whose tokens are to be accepted.
userinfourl	<String>	Read-write	URL to which OAuth access token will be posted to obtain user information.
certfilepath	<String>	Read-write	Path to the file that contains JWKs (Json Web Key) for JWT (Json Web Token) verification.
granttype	<String>	Read-write	Grant type support. value can be code or password.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: CODE Possible values = CODE, PASSWORD
authentication	<String>	Read-write	If authentication is disabled, password is not sent in the request. . Default value: ENABLED Possible values = ENABLED, DISABLED
introspecturl	<String>	Read-write	URL to which access token would be posted for validation.
allowedalgorithms	<String[]>	Read-write	Multivalued option to specify allowed token verification algorithms. . Default value: OAUTH_ALG_ALL Possible values = HS256, RS256, RS512, HS512
pkce	<String>	Read-write	Option to enable/ disable PKCE flow during authentication. . Default value: ENABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ENABLED, DISABLED
tokenendpointauthmethod	<String>	Read-write	Option to select the variant of token authentication method. This method is used while exchanging code with IdP. . Default value: client_secret_post, Possible values = client_secret_post, client_secret_jwt, private_key_jwt, client_secret_basic
metadataurl	<String>	Read-write	Well-known configuration endpoint of the Authorization Server. Citrix ADC fetches server details from this endpoint. .
resourceuri	<String>	Read-write	Resource URL for Oauth configuration.
requestattribute	<String>	Read-write	Name-Value pairs of attributes to be inserted in request parameter. Configuration format is name=value_expr@@@name2=value2_expr@@@.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			'@@@' is used as delimiter between Name-Value pairs. name is a literal string whose value is 127 characters and does not contain '=' character. Value is advanced policy expression terminated by @@@ delimiter. Last value need not contain the delimiter.
intunedeviceidexpression	<String>	Read-write	The expression that will be evaluated to obtain IntuneDeviceId for compliance check against IntuneNAC device compliance endpoint. The expression is applicable when the OAuthType is INTUNE. The maximum length allowed to be used as IntuneDeviceId for the device compliance check from the computed response after the expression evaluation is 41.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Examples: add authentication oauthAction <actionName> -intuneDeviceIdExpression 'AAA.LOGIN.INTUNEURI.AFTER_STR("IntuneDeviceId://")' .
scopes	<String>	Read-write	OAuth Scopes expected. Please specify scopes in space separated format as per RFC 6749 (OAuth 2.0). Each scope value can contain any printable ASCII character except double-quote (") and backslash (\). Maximum length is 1024. Maximum length = 1024
oauthstatus	<String>	Read-only	Describes status information of oauth server. Default value: INIT Possible values = INIT, CERTFETCH, AADFORGRAPH, GRAPH, AADFORMDM,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			MDMINFO, COMPLETE
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationoauthaction **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationoauthaction":{

<b>"name":<String_value>,

</b>"oauthtype":<String_value>,

"authorizationendpoint":<String_value>,

"tokenendpoint":<String_value>,

"idtokendecryptendpoint":<String_value>,

"clientid":<String_value>,

"clientsecret":<String_value>,

"defaultauthenticationgroup":<String_value>,

"oauthmiscflags":<String[]_value>,

"attribute1":<String_value>,

"attribute2":<String_value>,
```

```
"attribute3":<String_value>,

"attribute4":<String_value>,

"attribute5":<String_value>,

"attribute6":<String_value>,

"attribute7":<String_value>,

"attribute8":<String_value>,

"attribute9":<String_value>,

"attribute10":<String_value>,

"attribute11":<String_value>,

"attribute12":<String_value>,

"attribute13":<String_value>,

"attribute14":<String_value>,

"attribute15":<String_value>,

"attribute16":<String_value>,

"attributes":<String_value>,

"tenantid":<String_value>,

"graphendpoint":<String_value>,

"refreshinterval":<Integer_value>,

"certendpoint":<String_value>,

"audience":<String_value>,

"usernamefield":<String_value>,

"skewtime":<Integer_value>,
```

```
"issuer":<String_value>,

"userinfourl":<String_value>,

"certfilepath":<String_value>,

"granttype":<String_value>,

"authentication":<String_value>,

"introspecturl":<String_value>,

"allowedalgorithms":<String[]_value>,

"pkce":<String_value>,

"tokenendpointauthmethod":<String_value>,

"metadataurl":<String_value>,

"resourceuri":<String_value>,

"requestattribute":<String_value>,

"intunedeviceidexpression":<String_value>,

"scopes":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationoauthaction/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationoauthaction **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationoauthaction":{

<b>"name":<String_value>,

</b>"oauthtype":<String_value>,

"authorizationendpoint":<String_value>,

"tokenendpoint":<String_value>,

"idtokendecryptendpoint":<String_value>,

"clientid":<String_value>,

"clientsecret":<String_value>,

"defaultauthenticationgroup":<String_value>,

"oauthmiscflags":<String[]_value>,

"attribute1":<String_value>,

"attribute2":<String_value>,

"attribute3":<String_value>,
```

```
"attribute4":<String_value>,

"attribute5":<String_value>,

"attribute6":<String_value>,

"attribute7":<String_value>,

"attribute8":<String_value>,

"attribute9":<String_value>,

"attribute10":<String_value>,

"attribute11":<String_value>,

"attribute12":<String_value>,

"attribute13":<String_value>,

"attribute14":<String_value>,

"attribute15":<String_value>,

"attribute16":<String_value>,

"attributes":<String_value>,

"tenantid":<String_value>,

"graphendpoint":<String_value>,

"refreshinterval":<Integer_value>,

"certendpoint":<String_value>,

"audience":<String_value>,

"usernamefield":<String_value>,

"skewtime":<Integer_value>,

"issuer":<String_value>,
```

```
"userinfourl":<String_value>,

"certfilepath":<String_value>,

"granttype":<String_value>,

"authentication":<String_value>,

"introspecturl":<String_value>,

"allowedalgorithms":<String[]_value>,

"pkce":<String_value>,

"tokenendpointauthmethod":<String_value>,

"metadataurl":<String_value>,

"resourceuri":<String_value>,

"requestattribute":<String_value>,

"intunedeviceidexpression":<String_value>,

"scopes":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationoauthaction? **action=unset**
HTTP Method: POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationoauthaction":{

<b>"name":<String_value>,

</b>"oauthtype":true,

"idtokendecryptendpoint":true,

"defaultauthenticationgroup":true,

"oauthmiscflags":true,

"attribute1":true,

"attribute2":true,

"attribute3":true,

"attribute4":true,

"attribute5":true,

"attribute6":true,

"attribute7":true,

"attribute8":true,

"attribute9":true,

"attribute10":true,

"attribute11":true,

"attribute12":true,

"attribute13":true,

"attribute14":true,

"attribute15":true,
```

```
"attribute16":true,

"attributes":true,

"graphendpoint":true,

"refreshinterval":true,

"certendpoint":true,

"audience":true,

"usernamefield":true,

"skewtime":true,

"issuer":true,

"userinfourl":true,

"certfilepath":true,

"authentication":true,

"introspecturl":true,

"allowedalgorithms":true,

"pkce":true,

"tokenendpointauthmethod":true,

"metadataurl":true,

"resourceuri":true,

"requestattribute":true,

"intunedeviceidexpression":true,

"scopes":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationoauthaction **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/authenticationoauthaction? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/authenticationoauthaction? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of authenticationoauthaction resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/authenticationoauthaction? **view=summary**

Use this query-parameter to get the summary output of authenticationoauthaction resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/authenticationoauthaction? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authenticationoauthaction resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationoauthaction": [ {

"name":<String_value>,

"authorizationendpoint":<String_value>,

"tokenendpoint":<String_value>,

"idtokendecryptendpoint":<String_value>,

"clientid":<String_value>,

"clientsecret":<String_value>,

"defaultauthenticationgroup":<String_value>,

"oauthmiscflags":<String[]_value>,

"attribute1":<String_value>,

"attribute2":<String_value>,

"attribute3":<String_value>,

"attribute4":<String_value>,

"attribute5":<String_value>,

"attribute6":<String_value>,

"attribute7":<String_value>,

"attribute8":<String_value>,

"attribute9":<String_value>,

"attribute10":<String_value>,
```

```
"attribute11":<String_value>,

"attribute12":<String_value>,

"attribute13":<String_value>,

"attribute14":<String_value>,

"attribute15":<String_value>,

"attribute16":<String_value>,

"attributes":<String_value>,

"tenantid":<String_value>,

"graphendpoint":<String_value>,

"refreshinterval":<Integer_value>,

"certendpoint":<String_value>,

"oauthtype":<String_value>,

"audience":<String_value>,

"usernamefield":<String_value>,

"skewtime":<Integer_value>,

"issuer":<String_value>,

"oauthstatus":<String_value>,

"userinfourl":<String_value>,

"certfilepath":<String_value>,

"granttype":<String_value>,

"authentication":<String_value>,

"introspecturl":<String_value>,
```

```
"allowedalgorithms":<String[]_value>,

"pkce":<String_value>,

"tokenendpointauthmethod":<String_value>,

"metadataurl":<String_value>,

"resourceuri":<String_value>,

"requestattribute":<String_value>,

"intunedeviceidexpression":<String_value>,

"scopes":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationoauthaction/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/ authenticationoauthaction/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/authenticationoauthaction/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of authenticationoauthaction resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationoauthaction": [ {

"name":<String_value>,

"authorizationendpoint":<String_value>,

"tokenendpoint":<String_value>,

"idtokendecryptendpoint":<String_value>,

"clientid":<String_value>,

"clientsecret":<String_value>,

"defaultauthenticationgroup":<String_value>,

"oauthmiscflags":<String[]_value>,

"attribute1":<String_value>,

"attribute2":<String_value>,

"attribute3":<String_value>,

"attribute4":<String_value>,

"attribute5":<String_value>,

"attribute6":<String_value>,

"attribute7":<String_value>,

"attribute8":<String_value>,
```

```
"attribute9":<String_value>,

"attribute10":<String_value>,

"attribute11":<String_value>,

"attribute12":<String_value>,

"attribute13":<String_value>,

"attribute14":<String_value>,

"attribute15":<String_value>,

"attribute16":<String_value>,

"attributes":<String_value>,

"tenantid":<String_value>,

"graphendpoint":<String_value>,

"refreshinterval":<Integer_value>,

"certendpoint":<String_value>,

"oauthtype":<String_value>,

"audience":<String_value>,

"usernamefield":<String_value>,

"skewtime":<Integer_value>,

"issuer":<String_value>,

"oauthstatus":<String_value>,

"userinfourl":<String_value>,

"certfilepath":<String_value>,

"granttype":<String_value>,
```

```
"authentication":<String_value>,

"introspecturl":<String_value>,

"allowedalgorithms":<String[]_value>,

"pkce":<String_value>,

"tokenendpointauthmethod":<String_value>,

"metadataurl":<String_value>,

"resourceuri":<String_value>,

"requestattribute":<String_value>,

"intunedeviceidexpression":<String_value>,

"scopes":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationoauthaction? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationoauthaction": [ { "__count": "#no"} ] }
```

authenticationoauthidppolicy

Configuration for AAA OAuth IdentityProvider (IdP) policy resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the OAuth Identity Provider (IdP) authentication policy. This is used for configuring Citrix ADC as OAuth Identity Provider. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			name in double or single quotation marks (for example, "my policy" or 'my policy'). Minimum length = 1
rule	<String>	Read-write	Expression that the policy uses to determine whether to respond to the specified request. Minimum length = 1
action	<String>	Read-write	Name of the profile to apply to requests or connections that match this policy. Minimum length = 1
undefaction	<String>	Read-write	Action to perform if the result of policy evaluation is undefined (UNDEF). An UNDEF event indicates an internal error condition. Only DROP/RESET actions can be used.
comment	<String>	Read-write	Any comments to preserve information about this policy.
logaction	<String>	Read-write	Name of messagelog action to use when a request matches this policy.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
newname	<String>	Read-write	New name for the OAuth IdentityProvider policy. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space ( ), at (@), equals (=), colon (:), and underscore characters. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my oauthidppolicy policy" or 'my oauthidppolicy policy'). Minimum length = 1
gotopriorityexpression	<String>	Read-only	Expression specifying the priority of the next policy

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			which will get evaluated if the current policy rule evaluates to TRUE.
hits	<Integer>	Read-only	Number of hits.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT
- RENAME

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationoauthidppolicy **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationoauthidppolicy":{

<b>"name":<String_value>,

</b><b>"rule":<String_value>,

</b><b>"action":<String_value>,

</b>"undefaction":<String_value>,

"comment":<String_value>,

"logaction":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationoauthidppolicy/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationoauthidppolicy **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationoauthidppolicy":{

<b>"name":<String_value>,

</b>"rule":<String_value>,

"action":<String_value>,

"undefaction":<String_value>,

"comment":<String_value>,

"logaction":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationoauthidppolicy? **action=unset**
HTTP Method: POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationoauthidppolicy":{

<b>"name":<String_value>,

</b>"undefaction":true,

"comment":true,

"logaction":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

RENAME

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationoauthidppolicy? **action=rename**
HTTP Method: POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationoauthidppolicy":{

<b>"name":<String_value>,

</b><b>"newname":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationoauthidppolicy **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/authenticationoauthidppolicy? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/authenticationoauthidppolicy? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of authenticationoauthidppolicy resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/authenticationoauthidppolicy? **view=summary**

Use this query-parameter to get the summary output of authenticationoauthidppolicy resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/authenticationoauthidppolicy? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authenticationoauthidppolicy resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationoauthidppolicy": [ {

"name":<String_value>,

"rule":<String_value>,

"action":<String_value>,

"undefaction":<String_value>,

"comment":<String_value>,

"logaction":<String_value>,

"gotopriorityexpression":<String_value>,

"hits":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationoauthidppolicy/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/ authenticationoauthidppolicy/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/authenticationoauthidppolicy/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of authenticationoauthidppolicy resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationoauthidppolicy": [ {

"name":<String_value>,

"rule":<String_value>,

"action":<String_value>,

"undefaction":<String_value>,
```

```
"comment":<String_value>,

"logaction":<String_value>,

"gotopriorityexpression":<String_value>,

"hits":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationoauthidppolicy? **count=yes**
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationoauthidppolicy": [ { "__count": "#no"} ] }
```

authenticationoauthidppolicy_authenticationvserver_binding

Binding object showing the authenticationvserver that can be bound to authenticationoauthidppolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the OAuth IdentityProvider (IdP) policy for which to display detailed information. Minimum length = 1
boundto	<String>	Read-write	The entity name to which policy is bound.
priority	<Integer>	Read-only	.
activepolicy	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationoauthidppolicy_authenticationvserver_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ authenticationoauthidppolicy_authenticationvserver_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of authenticationoauthidppolicy_authenticationvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ authenticationoauthidppolicy_authenticationvserver_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authenticationoauthidppolicy_authenticationvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationoauthidppolicy_authenticationvserver_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"priority":<Integer_value>,

"activepolicy":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationoauthidppolicy_authenticationvserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ authenticationoauthidppolicy_authenticationvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationoauthidppolicy_authenticationvserver_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"priority":<Integer_value>,

"activepolicy":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationoauthidppolicy_authenticationvserver_binding/ name_value<String> ? **count=yes**
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"authenticationoauthidppolicy_authenticationvserver_binding":
[ { "__count": "#no"} ] }
```

authenticationoauthidppolicy_binding

Binding object which returns the resources bound to authenticationoauthidppolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the OAuth IdentityProvider (IdP) policy for which to display detailed information. Minimum length = 1
authenticationoauthidppolicy_authenticationvserver_binding	<authenticationoauthidppolicy_authenticationvserver_binding[]>	Read-only	authenticationvserver that can be bound to authenticationoauthidppolicy.
authenticationoauthidppolicy_vpnvserver_binding	<authenticationoauthidppolicy_vpnvserver_binding[]>	Read-only	vpnvserver that can be bound to authenticationoauthidppolicy.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationoauthidppolicy_binding/name_value<String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationoauthidppolicy_binding": [ {

"name":<String_value>,

"authenticationoauthidppolicy_authenticationvserver_binding":<authenticati
onoauthidppolicy_authenticationvserver_binding[]_value>,

"authenticationoauthidppolicy_vpnvserver_binding":<authenticationoauthidpp
olicy_vpnvserver_binding[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationoauthidppolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/authenticationoauthidppolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationoauthidppolicy_binding": [ {

"name":<String_value>,

"authenticationoauthidppolicy_authenticationvserver_binding":<authenticationoauthidppolicy_authenticationvserver_binding[]_value>,

"authenticationoauthidppolicy_vpnvserver_binding":<authenticationoauthidppolicy_vpnvserver_binding[]_value>

}]}
```

authenticationoauthidppolicy_vpnvserver_binding

Binding object showing the vpnvserver that can be bound to authenticationoauthidppolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
boundto	<String>	Read-write	The entity name to which policy is bound.
name	<String>	Read-write	Name of the OAuth IdentityProvider (IdP) policy for which to display detailed information. Minimum length = 1
activepolicy	<Integer>	Read-only	.
priority	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationoauthidppolicy_vpnvserver_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/authenticationoauthidppolicy_vpnvserver_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of authenticationoauthidppolicy_vpnvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ authenticationoauthidppolicy_vpnvserver_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authenticationoauthidppolicy_vpnvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationoauthidppolicy_vpnvserver_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"activepolicy":<Integer_value>,

"priority":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationoauthidppolicy_vpnvserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ authenticationoauthidppolicy_vpnvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationoauthidppolicy_vpnvserver_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"activepolicy":<Integer_value>,

"priority":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationoauthidppolicy_vpnvserver_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"authenticationoauthidppolicy_vpnvserver_binding": [ { "__count":
"#no"} ] }
```

authenticationoauthidpprofile

Configuration for OAuth Identity Provider (IdP) profile resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the new OAuth Identity Provider (IdP) single sign-on profile. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			characters. Cannot be changed after an action is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my action" or 'my action'). Minimum length = 1
clientid	<String>	Read-write	Unique identity of the relying party requesting for authentication. Minimum length = 1
clientsecret	<String>	Read-write	Unique secret string to authorize relying party at authorization server. Minimum length = 1
redirecturl	<String>	Read-write	URL endpoint on relying party to which the OAuth token is to be sent. Minimum length = 1
issuer	<String>	Read-write	The name to be used in requests sent from Citrix ADC to IdP to

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			uniquely identify Citrix ADC. Minimum length = 1
configservice	<String>	Read-write	Name of the entity that is used to obtain configuration for the current authentication request. It is used only in Citrix Cloud. Minimum length = 1
audience	<String>	Read-write	Audience for which token is being sent by Citrix ADC IdP. This is typically entity name or url that represents the recipient.
skewtime	<Integer>	Read-write	This option specifies the duration for which the token sent by Citrix ADC IdP is valid. For example, if skewTime is 10, then token would be valid from (current time - 10) min to (current time + 10) min, ie 20min in all. Default value: 5
defaultauthentication group	<String>	Read-write	This group will be part of AAA session's internal group list. This will be helpful to admin in Nfactor flow to decide right AAA configuration for

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Relaying Party. In authentication policy AAA.USER.IS_MEMBER_OF("<default_auth_group>") is way to use this feature.
relyingpartymetadataurl	<String>	Read-write	This is the endpoint at which Citrix ADC IdP can get details about Relying Party (RP) being configured. Metadata response should include endpoints for jwks_uri for RP public key(s).
refreshinterval	<Integer>	Read-write	Interval at which Relying Party metadata is refreshed. Default value: 50
encrypttoken	<String>	Read-write	Option to encrypt token when Citrix ADC IDP sends one. Default value: OFF Possible values = ON, OFF
signatureservice	<String>	Read-write	Name of the service in cloud used to sign the data. This is applicable only if signature if offloaded to cloud. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
signaturealg	<String>	Read-write	Algorithm to be used to sign OpenID tokens. Default value: RS256 Possible values = RS256, RS512
attributes	<String>	Read-write	Name-Value pairs of attributes to be inserted in idtoken. Configuration format is name=value_expr@@@name2=value2_expr@@@. '@@@' is used as delimiter between Name-Value pairs. name is a literal string whose value is 127 characters and does not contain '=' character. Value is advanced policy expression terminated by @@@ delimiter. Last value need not contain the delimiter.
sendpassword	<String>	Read-write	Option to send encrypted password in idtoken.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: OFF Possible values = ON, OFF
oauthstatus	<String>	Read-only	Describes status information of oauth idp metadata fetch process. Default value: INIT Possible values = INIT, CERTFETCH, AADFORGRAPH, GRAPH, AADFORMDM, MDMINFO, COMPLETE
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationoauthidpprofile **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationoauthidpprofile":{

<b>"name":<String_value>,

</b>"clientid":<String_value>,
```

```
"clientsecret":<String_value>,

"redirecturl":<String_value>,

"issuer":<String_value>,

"configservice":<String_value>,

"audience":<String_value>,

"skewtime":<Integer_value>,

"defaultauthenticationgroup":<String_value>,

"relyingpartymetadataurl":<String_value>,

"refreshinterval":<Integer_value>,

"encrypttoken":<String_value>,

"signatureservice":<String_value>,

"signaturealg":<String_value>,

"attributes":<String_value>,

"sendpassword":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationoauthidpprofile/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationoauthidpprofile **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationoauthidpprofile":{

<b>"name":<String_value>,

</b>"clientid":<String_value>,

"clientsecret":<String_value>,

"redirecturl":<String_value>,

"issuer":<String_value>,

"configservice":<String_value>,

"audience":<String_value>,

"skewtime":<Integer_value>,

"defaultauthenticationgroup":<String_value>,

"relyingpartymetadataurl":<String_value>,

"refreshinterval":<Integer_value>,

"encrypttoken":<String_value>,
```

```
"signatureservice":<String_value>,

"signaturealg":<String_value>,

"attributes":<String_value>,

"sendpassword":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationoauthidpprofile? **action=unset**
HTTP Method: POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationoauthidpprofile":{

<b>"name":<String_value>,

</b>"issuer":true,

"configservice":true,

"audience":true,

"skewtime":true,

"defaultauthenticationgroup":true,
```

```
"relyingpartymetadataurl":true,

"refreshinterval":true,

"encrypttoken":true,

"signatureservice":true,

"signaturealg":true,

"attributes":true,

"sendpassword":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationoauthidpprofile **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/authenticationoauthidpprofile? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/authenticationoauthidpprofile? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of authenticationoauthidpprofile resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/authenticationoauthidpprofile? **view=summary**

Use this query-parameter to get the summary output of authenticationoauthidpprofile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/authenticationoauthidpprofile? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authenticationoauthidpprofile resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationoauthidpprofile": [ {

"name":<String_value>,

"clientid":<String_value>,

"clientsecret":<String_value>,

"redirecturl":<String_value>,

"issuer":<String_value>,

"configservice":<String_value>,

"audience":<String_value>,

"skewtime":<Integer_value>,

"defaultauthenticationgroup":<String_value>,
```

```
"relyingpartymetadataurl":<String_value>,

"refreshinterval":<Integer_value>,

"encrypttoken":<String_value>,

"signatureservice":<String_value>,

"signaturealg":<String_value>,

"oauthstatus":<String_value>,

"attributes":<String_value>,

"sendpassword":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationoauthidpprofile/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/ authenticationoauthidpprofile/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/authenticationoauthidpprofile/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of authenticationoauthidpprofile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationoauthidpprofile": [ {

"name":<String_value>,

"clientid":<String_value>,

"clientsecret":<String_value>,

"redirecturl":<String_value>,

"issuer":<String_value>,

"configservice":<String_value>,

"audience":<String_value>,

"skewtime":<Integer_value>,

"defaultauthenticationgroup":<String_value>,

"relyingpartymetadataurl":<String_value>,

"refreshinterval":<Integer_value>,

"encrypttoken":<String_value>,

"signatureservice":<String_value>,

"signaturealg":<String_value>,

"oauthstatus":<String_value>,

"attributes":<String_value>,
```

```
"sendpassword":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationoauthidpprofile? **count=yes**
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationoauthidpprofile": [ { "__count": "#no"} ] }
```

authenticationpolicy

Configuration for Authentication Policy resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the advance

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			AUTHENTICATION policy. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after AUTHENTICATION policy is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my authentication policy" or 'my authentication policy'). Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
rule	<String>	Read-write	Name of the Citrix ADC named rule, or an expression, that the policy uses to determine whether to attempt to authenticate the user with the AUTHENTICATION server.
action	<String>	Read-write	Name of the authentication action to be performed if the policy matches.
undefaction	<String>	Read-write	Action to perform if the result of policy evaluation is undefined (UNDEF). An UNDEF event indicates an internal error condition. Only the above built-in actions can be used.
comment	<String>	Read-write	Any comments to preserve information about this policy.
logaction	<String>	Read-write	Name of messagelog action to use when a request matches this policy.
newname	<String>	Read-write	New name for the authentication policy. Must begin with a letter, number, or the underscore character (_), and must contain

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			only letters, numbers, and the hyphen (-), period (.) hash (#), space ( ), at (@), equals (=), colon (:), and underscore characters. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my authentication policy" or 'my authentication policy'). Minimum length = 1
hits	<Integer>	Read-only	Number of hits.
description	<String>	Read-only	Description of the policy.
policysubtype	<String>	Read-only	. Possible values = LOCAL, RADIUS, LDAP, TACACS, CERT, NEGOTIATE, SAML, PROFILE, DFA, SAMLIDP,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			WEBAUTH, OAUTH, NO_AUTHN, EPA, SFAUTH, AZUREVAULT, EMAIL, CAPTCHA, ASSIGNMENT, PROTECTED_USER
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT
- RENAME

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationpolicy **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationpolicy":{

<b>"name":<String_value>,

</b><b>"rule":<String_value>,

</b><b>"action":<String_value>,

</b>"undefaction":<String_value>,

"comment":<String_value>,

"logaction":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationpolicy/ name_value<String>
HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationpolicy **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationpolicy":{

<b>"name":<String_value>,

</b>"rule":<String_value>,

"action":<String_value>,

"undefaction":<String_value>,

"comment":<String_value>,

"logaction":<String_value>
```

```
}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationpolicy? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationpolicy":{

<b>"name":<String_value>,

</b>"undefaction":true,

"comment":true,

"logaction":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

RENAME

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationpolicy? **action=rename HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationpolicy":{

<b>"name":<String_value>,

</b><b>"newname":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationpolicy **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/authenticationpolicy? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/authenticationpolicy? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of authenticationpolicy resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/authenticationpolicy? **view=summary**

Use this query-parameter to get the summary output of authenticationpolicy resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/authenticationpolicy? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authenticationpolicy resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationpolicy": [ {

"name":<String_value>,

"rule":<String_value>,

"action":<String_value>,

"undefaction":<String_value>,

"comment":<String_value>,

"logaction":<String_value>,

"hits":<Integer_value>,

"description":<String_value>,

"policysubtype":<String_value>,
```

```
"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationpolicy/ name_value<String>
Query-parameters: attrs http:// <netscaler-ip-address> /nitro/v1/config/authenticationpolicy/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/authenticationpolicy/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of authenticationpolicy resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationpolicy": [ {

"name":<String_value>,
```

```
"rule":<String_value>,

"action":<String_value>,

"undefaction":<String_value>,

"comment":<String_value>,

"logaction":<String_value>,

"hits":<Integer_value>,

"description":<String_value>,

"policysubtype":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationpolicy? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationpolicy": [ { "__count": "#no"} ] }
```

authenticationpolicy_authenticationpolicylabel_binding

Binding object showing the authenticationpolicylabel that can be bound to authenticationpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
boundto	<String>	Read-write	The entity name to which policy is bound.
name	<String>	Read-write	Name of the advance authentication policy. Minimum length = 1
activepolicy	<Integer>	Read-only	.
gotopriorityexpression	<String>	Read-only	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
nextfactor	<String>	Read-only	On success invoke label.
priority	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET

- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationpolicy_authenticationpolicylabel_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ authenticationpolicy_authenticationpolicylabel_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of authenticationpolicy_authenticationpolicylabel_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ authenticationpolicy_authenticationpolicylabel_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authenticationpolicy_authenticationpolicylabel_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationpolicy_authenticationpolicylabel_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"activepolicy":<Integer_value>,

"gotopriorityexpression":<String_value>,

"nextfactor":<String_value>,

"priority":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationpolicy_authenticationpolicylabel_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ authenticationpolicy_authenticationpolicylabel_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationpolicy_authenticationpolicylabel_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"activepolicy":<Integer_value>,

"gotopriorityexpression":<String_value>,

"nextfactor":<String_value>,

"priority":<Integer_value>

}]}
```

```
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationpolicy_authenticationpolicylabel_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"authenticationpolicy_authenticationpolicylabel_binding": [ { "__count": "#no"} ] }
```

authenticationpolicy_authenticationvserver_binding

Binding object showing the authenticationvserver that can be bound to authenticationpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the advance authentication policy. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
boundto	<String>	Read-write	The entity name to which policy is bound.
priority	<Integer>	Read-only	.
nextfactor	<String>	Read-only	On success invoke label.
gotopriorityexpression	<String>	Read-only	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
activepolicy	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationpolicy_authenticationvserver_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ authenticationpolicy_authenticationvserver_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of authenticationpolicy_authenticationvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ authenticationpolicy_authenticationvserver_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authenticationpolicy_authenticationvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationpolicy_authenticationvserver_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"priority":<Integer_value>,

"nextfactor":<String_value>,

"gotopriorityexpression":<String_value>,

"activepolicy":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationpolicy_authenticationvserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ authenticationpolicy_authenticationvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationpolicy_authenticationvserver_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"priority":<Integer_value>,

"nextfactor":<String_value>,

"gotopriorityexpression":<String_value>,

"activepolicy":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationpolicy_authenticationvserver_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"authenticationpolicy_authenticationvserver_binding": [ { "__count":
"#no"} ] }
```

authenticationpolicy_binding

Binding object which returns the resources bound to authenticationpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the advance authentication policy. Minimum length = 1
authenticationpolicy_authenticationvserver_binding	<authenticationpolicy_authenticationvserver_binding[]>	Read-only	authenticationvserver that can be bound to authenticationpolicy.
authenticationpolicy_systemglobal_binding	<authenticationpolicy_systemglobal_binding[]>	Read-only	systemglobal that can be bound to authenticationpolicy.
authenticationpolicy_authenticationpolicylabel_binding	<authenticationpolicy_authenticationpolicylabel_binding[]>	Read-only	authenticationpolicylabel that can be bound to authenticationpolicy.

Operations

(click to see Properties)

- GET

- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationpolicy_binding/name_value<String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationpolicy_binding": [ {

"name":<String_value>,

"authenticationpolicy_authenticationvserver_binding":<authenticationpolicy
_authenticationvserver_binding[]_value>,

"authenticationpolicy_authenticationpolicylabel_binding":<authenticationpo
licy_authenticationpolicylabel_binding[]_value>,

"authenticationpolicy_systemglobal_binding":<authenticationpolicy_systemgl
obal_binding[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationpolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/authenticationpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationpolicy_binding": [ {

"name":<String_value>,

"authenticationpolicy_authenticationvserver_binding":<authenticationpolicy
_authenticationvserver_binding[]_value>,

"authenticationpolicy_authenticationpolicylabel_binding":<authenticationpo
licy_authenticationpolicylabel_binding[]_value>,

"authenticationpolicy_systemglobal_binding":<authenticationpolicy_systemgl
obal_binding[]_value>

}]}
```

authenticationpolicy_systemglobal_binding

Binding object showing the systemglobal that can be bound to authenticationpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the advance authentication policy. Minimum length = 1
boundto	<String>	Read-write	The entity name to which policy is bound.
priority	<Integer>	Read-only	.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
nextfactor	<String>	Read-only	On success invoke label.
gotopriorityexpression	<String>	Read-only	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
activepolicy	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationpolicy_systemglobal_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ authenticationpolicy_systemglobal_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of authenticationpolicy_systemglobal_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ authenticationpolicy_systemglobal_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authenticationpolicy_systemglobal_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationpolicy_systemglobal_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"priority":<Integer_value>,

"nextfactor":<String_value>,

"gotopriorityexpression":<String_value>,

"activepolicy":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationpolicy_systemglobal_binding
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/authenticationpolicy_systemglobal_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationpolicy_systemglobal_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"priority":<Integer_value>,

"nextfactor":<String_value>,

"gotopriorityexpression":<String_value>,

"activepolicy":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationpolicy_systemglobal_binding/name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"authenticationpolicy_systemglobal_binding": [ { "__count": "#no"} ] }
```

authenticationpolicylabel

Configuration for authentication policy label resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
labelname	<String>	Read-write	Name for the new authentication policy label. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my authentication policy label" or 'authentication policy label').

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
type	<String>	Read-write	Type of feature (aaatm or rba) against which to match the policies bound to this policy label. Default value: AAATM_REQ Possible values = AAATM_REQ, RBA_REQ
comment	<String>	Read-write	Any comments to preserve information about this authentication policy label.
loginschema	<String>	Read-write	Login schema associated with authentication policy label. Login schema defines the UI rendering by providing customization option of the fields. If user intervention is not needed for a given factor such as group extraction, a loginSchema whose authentication schema is "noschema" should be used.
newname	<String>	Read-write	The new name of the auth policy label.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum length = 1
numpol	<Integer>	Read-only	Number of polices bound to label.
hits	<Integer>	Read-only	Number of times policy label was invoked.
policyname	<String>	Read-only	Name of the authentication policy to bind to the policy label.
priority	<Integer>	Read-only	Specifies the priority of the policy.
gotopriorityexpression	<String>	Read-only	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
flowtype	<Integer>	Read-only	Flowtype of the bound authentication policy.
description	<String>	Read-only	Description of the policylabel.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE

- RENAME
- GET (ALL)
- GET
- COUNT
- UPDATE
- UNSET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationpolicylabel **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationpolicylabel":{

<b>"labelname":<String_value>,

</b>"type":<String_value>,

"comment":<String_value>,

"loginschema":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationpolicylabel/ labelname_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

RENAME

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationpolicylabel? **action=rename** **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationpolicylabel":{

<b>"labelname":<String_value>,

</b><b>"newname":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationpolicylabel **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationpolicylabel":{

<b>"labelname":<String_value>,

</b>"loginschema":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationpolicylabel? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationpolicylabel":{

<b>"labelname":<String_value>,

</b>"loginschema":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationpolicylabel **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/authenticationpolicylabel? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/authenticationpolicylabel? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of authenticationpolicylabel resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/authenticationpolicylabel? **view=summary**

Use this query-parameter to get the summary output of authenticationpolicylabel resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/authenticationpolicylabel? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authenticationpolicylabel resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationpolicylabel": [ {

"labelname":<String_value>,

"numpol":<Integer_value>,

"hits":<Integer_value>,

"policyname":<String_value>,

"priority":<Integer_value>,

"gotopriorityexpression":<String_value>,

"flowtype":<Integer_value>,

"description":<String_value>,

"comment":<String_value>,
```

```
"loginschema":<String_value>,

"type":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationpolicylabel/ labelname_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/ authenticationpolicylabel/ labelname_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/authenticationpolicylabel/ labelname_value<String> ? **view=summary**

Use this query-parameter to get the summary output of authenticationpolicylabel resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationpolicylabel": [ {

"labelname":<String_value>,

"numpol":<Integer_value>,

"hits":<Integer_value>,

"policyname":<String_value>,

"priority":<Integer_value>,

"gotopriorityexpression":<String_value>,

"flowtype":<Integer_value>,

"description":<String_value>,

"comment":<String_value>,

"loginschema":<String_value>,

"type":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationpolicylabel? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationpolicylabel": [ { "__count": "#no"} ] }
```

authenticationpolicylabel_authenticationpolicy_binding

Binding object showing the authenticationpolicy that can be bound to authenticationpolicylabel.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
priority	<Integer>	Read-write	Specifies the priority of the policy.
labelname	<String>	Read-write	Name of the authentication policy label to which to bind the policy.
nextfactor	<String>	Read-write	On success invoke label.
gotopriorityexpression	<String>	Read-write	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
policyname	<String>	Read-write	Name of the authentication policy to bind to the policy label.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/ authenticationpolicylabel_authenticationpolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"authenticationpolicylabel_authenticationpolicy_binding":{

<b>"labelname":<String_value>,

</b><b>"policyname":<String_value>,

</b><b>"priority":<Integer_value>,

</b>"gotopriorityexpression":<String_value>,

"nextfactor":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationpolicylabel_authenticationpolicy_binding/ labelname_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ authenticationpolicylabel_authenticationpolicy_binding/ labelname_value<String> ? **args= policyname:<String_value>, priority: <Integer_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationpolicylabel_authenticationpolicy_binding/ labelname_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ authenticationpolicylabel_authenticationpolicy_binding/ labelname_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of authenticationpolicylabel_authenticationpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ authenticationpolicylabel_authenticationpolicy_binding/ labelname_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authenticationpolicylabel_authenticationpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationpolicylabel_authenticationpolicy_binding": [ {

"priority":<Integer_value>,
```

```
"labelname":<String_value>,

"nextfactor":<String_value>,

"gotopriorityexpression":<String_value>,

"policyname":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationpolicylabel_authenticationpolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ authenticationpolicylabel_authenticationpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationpolicylabel_authenticationpolicy_binding": [ {

"priority":<Integer_value>,
```

```
"labelname":<String_value>,

"nextfactor":<String_value>,

"gotopriorityexpression":<String_value>,

"policyname":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationpolicylabel_authenticationpolicy_binding/ labelname_value<String> ? **count=yes**
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"authenticationpolicylabel_authenticationpolicy_binding": [ { "__count":
"#no"} ] }
```

authenticationpolicylabel_binding

Binding object which returns the resources bound to authenticationpolicylabel.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
labelname	<String>	Read-write	Name of the authorization policy label.
authenticationpolicylabel_authenticationpolicy_binding	<authenticationpolicylabel_authenticationpolicy_binding[]>	Read-only	authenticationpolicy that can be bound to authenticationpolicylabel.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationpolicylabel_binding/ labelname_value<String>

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationpolicylabel_binding": [ {

"labelname":<String_value>,

"authenticationpolicylabel_authenticationpolicy_binding":<authenticationpo
licylabel_authenticationpolicy_binding[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationpolicylabel_binding

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters:

bulkbindings

http:// <netscaler-ip-address> /nitro/v1/config/authenticationpolicylabel_binding?**bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationpolicylabel_binding": [ {

"labelname":<String_value>,

"authenticationpolicylabel_authenticationpolicy_binding":<authenticationpo
licylabel_authenticationpolicy_binding[]_value>

}]}
```

authenticationprotecteduseraction

Configuration for Protected user action resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the action to configure. Minimum length = 1
realmstr	<String>	Read-write	Kerberos Realm.
maxconcurrentusers	<Integer>	Read-write	Max number of concurrent users allowed. Default value: 8 Minimum value = 1 Maximum value = 512
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET

- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationprotecteduseraction **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationprotecteduseraction":{

<b>"name":<String_value>,

</b><b>"realmstr":<String_value>,

</b>"maxconcurrentusers":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationprotecteduseraction/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationprotecteduseraction **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationprotecteduseraction":{

<b>"name":<String_value>,

</b>"realmstr":<String_value>,

"maxconcurrentusers":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationprotecteduseraction?**action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationprotecteduseraction":{

<b>"name":<String_value>,

</b>"maxconcurrentusers":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationprotecteduseraction **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/ authenticationprotecteduseraction? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/authenticationprotecteduseraction? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of authenticationprotecteduseraction resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/authenticationprotecteduseraction? **view=summary**

Use this query-parameter to get the summary output of authenticationprotecteduseraction resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/authenticationprotecteduseraction? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authenticationprotecteduseraction resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationprotecteduseraction": [ {

"name":<String_value>,

"realmstr":<String_value>,

"maxconcurrentusers":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationprotecteduseraction/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/ authenticationprotecteduseraction/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/authenticationprotecteduseraction/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of authenticationprotecteduseraction resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationprotecteduseraction": [ {

"name":<String_value>,

"realmstr":<String_value>,

"maxconcurrentusers":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationprotecteduseraction? **count=yes**
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationprotecteduseraction": [ { "__count": "#no"} ] }
```

authenticationpushservice

Configuration for Service details for sending push notifications resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the push service. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at sign (@), equal sign (=), and hyphen (-) characters. Cannot be changed after the profile is created. CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my push service" or 'my push service'). . Minimum length = 1 Maximum length = 127
clientid	<String>	Read-write	Unique identity for communicating with

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Citrix Push server in cloud. Minimum length = 1
clientsecret	<String>	Read-write	Unique secret for communicating with Citrix Push server in cloud. Minimum length = 1
customerid	<String>	Read-write	Customer id/name of the account in cloud that is used to create clientid/secret pair. Minimum length = 1
refreshinterval	<Integer>	Read-write	Interval at which certificates or idtoken is refreshed. Default value: 50
Namespace	<String>	Read-only	This is fully qualified domain name of the notification service in the cloud. If omitted, namespace defaults to https://mfa.cloud.com/. Minimum length = 1 Maximum length = 63
hubname	<String>	Read-only	Name of the hub within a namespace. This is used to classify different identities within a namespace. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
servicekey	<String>	Read-only	Key to be used to compute signature necessary for registering to notification service. Minimum length = 1
servicekeyname	<String>	Read-only	Friendly name of the Key to be used to compute signature necessary for registering to notification service. Minimum length = 1
certendpoint	<String>	Read-only	URL of the endpoint that contains JWKs (Json Web Key) for JWT (Json Web Token) verification. This is used at cloud instance that offers push service.
pushservicestatus	<String>	Read-only	Describes status of push service. Default value: INIT Possible values = INIT, CERTFETCH, CCTOKEN, COMPLETE
trustservice	<String>	Read-only	URL of the service that generates tokens for cloud access. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
pushcloudserverstatus	<String>	Read-only	Describes status of the cloud service that does push. Possible values = UP, DOWN
signingkeyname	<String>	Read-only	Friendly name of the Key to be used to compute signature necessary for accessing notification service. Minimum length = 1
signingkey	<String>	Read-only	Key to be used to compute signature necessary for accessing notification service. Minimum length = 1
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationpushservice **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationpushservice":{

<b>"name":<String_value>,

</b>"clientid":<String_value>,
```

```
"clientsecret":<String_value>,

"customerid":<String_value>,

"refreshinterval":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationpushservice/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationpushservice **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationpushservice":{

<b>"name":<String_value>,

</b>"clientid":<String_value>,
```

```
"clientsecret":<String_value>,

"customerid":<String_value>,

"refreshinterval":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationpushservice? **action=unset**
HTTP Method: POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationpushservice":{

<b>"name":<String_value>,

</b>"refreshinterval":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationpushservice **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/authenticationpushservice? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/authenticationpushservice? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of authenticationpushservice resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/authenticationpushservice? **view=summary**

Use this query-parameter to get the summary output of authenticationpushservice resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/authenticationpushservice? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authenticationpushservice resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationpushservice": [ {

"name":<String_value>,

"Namespace":<String_value>,

"hubname":<String_value>,

"servicekey":<String_value>,

"servicekeyname":<String_value>,

"clientid":<String_value>,

"clientsecret":<String_value>,

"customerid":<String_value>,

"certendpoint":<String_value>,

"refreshinterval":<Integer_value>,

"pushservicestatus":<String_value>,

"trustservice":<String_value>,

"pushcloudserverstatus":<String_value>,

"signingkeyname":<String_value>,

"signingkey":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationpushservice/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/ authenticationpushservice/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/authenticationpushservice/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of authenticationpushservice resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationpushservice": [ {

"name":<String_value>,

"Namespace":<String_value>,

"hubname":<String_value>,

"servicekey":<String_value>,

"servicekeyname":<String_value>,

"clientid":<String_value>,

"clientsecret":<String_value>,
```

```
"customerid":<String_value>,

"certendpoint":<String_value>,

"refreshinterval":<Integer_value>,

"pushservicestatus":<String_value>,

"trustservice":<String_value>,

"pushcloudserverstatus":<String_value>,

"signingkeyname":<String_value>,

"signingkey":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationpushservice? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationpushservice": [ { "__count": "#no"} ] }
```

authenticationradiusaction

Configuration for RADIUS action resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the RADIUS action. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after the RADIUS action is added. Minimum length = 1
serverip	<String>	Read-write	IP address assigned to the RADIUS server. Minimum length = 1
servername	<String>	Read-write	RADIUS server name as a FQDN. Mutually exclusive

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			with RADIUS IP address. Minimum length = 1
serverport	<Integer>	Read-write	Port number on which the RADIUS server listens for connections. Minimum value = 1
authtimeout	<Integer>	Read-write	Number of seconds the Citrix ADC waits for a response from the RADIUS server. Default value: 3 Minimum value = 1
radkey	<String>	Read-write	Key shared between the RADIUS server and the Citrix ADC. Required to allow the Citrix ADC to communicate with the RADIUS server. Minimum length = 1
radnasip	<String>	Read-write	If enabled, the Citrix ADC IP address (NSIP) is sent to the RADIUS server as the Network Access Server IP (NASIP) address. The RADIUS protocol defines the meaning and use of the NASIP address.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ENABLED, DISABLED
radnasid	<String>	Read-write	If configured, this string is sent to the RADIUS server as the Network Access Server ID (NASID).
radvendorid	<Integer>	Read-write	RADIUS vendor ID attribute, used for RADIUS group extraction. Minimum value = 1
radattributetype	<Integer>	Read-write	RADIUS attribute type, used for RADIUS group extraction. Minimum value = 1
radgroupsprefix	<String>	Read-write	RADIUS groups prefix string. This groups prefix precedes the group names within a RADIUS attribute for RADIUS group extraction.
radgroupseparator	<String>	Read-write	RADIUS group separator string The group separator delimits group names within a RADIUS attribute for RADIUS group extraction.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
passencoding	<String>	Read-write	Encoding type for passwords in RADIUS packets that the Citrix ADC sends to the RADIUS server. Default value: pap Possible values = pap, chap, mschapv1, mschapv2
ipvendorid	<Integer>	Read-write	Vendor ID of the intranet IP attribute in the RADIUS response. NOTE: A value of 0 indicates that the attribute is not vendor encoded.
ipattributetype	<Integer>	Read-write	Remote IP address attribute type in a RADIUS response. Minimum value = 1
accounting	<String>	Read-write	Whether the RADIUS server is currently accepting accounting messages. Possible values = ON, OFF
pwdvendorid	<Integer>	Read-write	Vendor ID of the attribute, in the RADIUS response,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			used to extract the user password. Minimum value = 1
pwdattributetype	<Integer>	Read-write	Vendor-specific password attribute type in a RADIUS response. Minimum value = 1
defaultauthentication group	<String>	Read-write	This is the default group that is chosen when the authentication succeeds in addition to extracted groups.
callingstationid	<String>	Read-write	Send Calling-Station-ID of the client to the RADIUS server. IP Address of the client is sent as its Calling-Station-ID. Default value: DISABLED Possible values = ENABLED, DISABLED
authservretry	<Integer>	Read-write	Number of retry by the Citrix ADC before getting response from the RADIUS server. Default value: 3 Minimum value = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum value = 10
authentication	<String>	Read-write	Configure the RADIUS server state to accept or refuse authentication messages. Default value: ON Possible values = ON, OFF
tunnelendpointclientip	<String>	Read-write	Send Tunnel Endpoint Client IP address to the RADIUS server. Default value: DISABLED Possible values = ENABLED, DISABLED
transport	<String>	Read-write	Transport mode to RADIUS server. Default value: RAD_TRANSPORT_UDP Possible values = UDP, TCP, TLS
targetlbvserver	<String>	Read-write	If transport mode is TLS, specify the name of LB vserver to associate. The LB vserver needs to be of type TCP and service associated

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			needs to be SSL_TCP.
messageauthenticator	<String>	Read-write	Control whether the Message-Authenticator attribute is included in a RADIUS Access-Request packet. Default value: ON Possible values = ON, OFF
ipaddress	<String>	Read-only	IP address.
success	<Integer>	Read-only	.
failure	<Integer>	Read-only	.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationradiusaction **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationradiusaction":{

<b>"name":<String_value>,

</b>"serverip":<String_value>,
```

```
"servername":<String_value>,

"serverport":<Integer_value>,

"authtimeout":<Integer_value>,

<b>"radkey":<String_value>,

</b>"radnasip":<String_value>,

"radnasid":<String_value>,

"radvendorid":<Integer_value>,

"radattributetype":<Integer_value>,

"radgroupsprefix":<String_value>,

"radgroupseparator":<String_value>,

"passencoding":<String_value>,

"ipvendorid":<Integer_value>,

"ipattributetype":<Integer_value>,

"accounting":<String_value>,

"pwdvendorid":<Integer_value>,

"pwdattributetype":<Integer_value>,

"defaultauthenticationgroup":<String_value>,

"callingstationid":<String_value>,

"authservretry":<Integer_value>,

"authentication":<String_value>,

"tunnelendpointclientip":<String_value>,

"transport":<String_value>,
```

```
"targetlbvserver":<String_value>,

"messageauthenticator":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationradiusaction/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationradiusaction **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationradiusaction":{

<b>"name":<String_value>,

</b>"serverip":<String_value>,

"servername":<String_value>,
```

```
"serverport":<Integer_value>,

"authtimeout":<Integer_value>,

"radkey":<String_value>,

"radnasip":<String_value>,

"radnasid":<String_value>,

"radvendorid":<Integer_value>,

"radattributetype":<Integer_value>,

"radgroupsprefix":<String_value>,

"radgroupseparator":<String_value>,

"passencoding":<String_value>,

"ipvendorid":<Integer_value>,

"ipattributetype":<Integer_value>,

"accounting":<String_value>,

"pwdvendorid":<Integer_value>,

"pwdattributetype":<Integer_value>,

"defaultauthenticationgroup":<String_value>,

"callingstationid":<String_value>,

"authservretry":<Integer_value>,

"authentication":<String_value>,

"tunnelendpointclientip":<String_value>,

"transport":<String_value>,

"targetlbvserver":<String_value>,
```

```
"messageauthenticator":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationradiusaction? **action=unset**
HTTP Method: POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationradiusaction":{

<b>"name":<String_value>,

</b>"serverport":true,

"authtimeout":true,

"radnasip":true,

"radnasid":true,

"radvendorid":true,

"radattributetype":true,

"radgroupsprefix":true,

"radgroupseparator":true,
```

```
"passencoding":true,

"ipvendorid":true,

"ipattributetype":true,

"accounting":true,

"pwdvendorid":true,

"pwdattributetype":true,

"defaultauthenticationgroup":true,

"callingstationid":true,

"authservretry":true,

"authentication":true,

"tunnelendpointclientip":true,

"transport":true,

"targetlbvserver":true,

"messageauthenticator":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationradiusaction **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/authenticationradiusaction? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/authenticationradiusaction? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of authenticationradiusaction resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/authenticationradiusaction? **view=summary**

Use this query-parameter to get the summary output of authenticationradiusaction resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/authenticationradiusaction? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authenticationradiusaction resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationradiusaction": [ {

"name":<String_value>,

"serverip":<String_value>,

"servername":<String_value>,
```

```
"serverport":<Integer_value>,

"authtimeout":<Integer_value>,

"radkey":<String_value>,

"radnasip":<String_value>,

"ipaddress":<String_value>,

"radnasid":<String_value>,

"radvendorid":<Integer_value>,

"radattributetype":<Integer_value>,

"radgroupsprefix":<String_value>,

"radgroupseparator":<String_value>,

"passencoding":<String_value>,

"ipvendorid":<Integer_value>,

"ipattributetype":<Integer_value>,

"accounting":<String_value>,

"success":<Integer_value>,

"failure":<Integer_value>,

"pwdvendorid":<Integer_value>,

"pwdattributetype":<Integer_value>,

"defaultauthenticationgroup":<String_value>,

"callingstationid":<String_value>,

"authservretry":<Integer_value>,

"authentication":<String_value>,
```

```
"tunnelendpointclientip":<String_value>,

"transport":<String_value>,

"targetlbvserver":<String_value>,

"messageauthenticator":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationradiusaction/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/ authenticationradiusaction/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/authenticationradiusaction/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of authenticationradiusaction resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationradiusaction": [ {

"name":<String_value>,

"serverip":<String_value>,

"servername":<String_value>,

"serverport":<Integer_value>,

"authtimeout":<Integer_value>,

"radkey":<String_value>,

"radnasip":<String_value>,

"ipaddress":<String_value>,

"radnasid":<String_value>,

"radvendorid":<Integer_value>,

"radattributetype":<Integer_value>,

"radgroupsprefix":<String_value>,

"radgroupseparator":<String_value>,

"passencoding":<String_value>,

"ipvendorid":<Integer_value>,

"ipattributetype":<Integer_value>,

"accounting":<String_value>,

"success":<Integer_value>,

"failure":<Integer_value>,
```

```
"pwdvendorid":<Integer_value>,

"pwdattributetype":<Integer_value>,

"defaultauthenticationgroup":<String_value>,

"callingstationid":<String_value>,

"authservretry":<Integer_value>,

"authentication":<String_value>,

"tunnelendpointclientip":<String_value>,

"transport":<String_value>,

"targetlbvserver":<String_value>,

"messageauthenticator":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationradiusaction? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationradiusaction": [ { "__count": "#no"} ] }
```

authenticationradiuspolicy

Configuration for RADIUS policy resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the RADIUS authentication policy. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after RADIUS policy is created. The following requirement applies only to the Citrix ADC CLI:

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my authentication policy" or 'my authentication policy'). Minimum length = 1
rule	<String>	Read-write	Name of the Citrix ADC named rule, or an expression, that the policy uses to determine whether to attempt to authenticate the user with the RADIUS server.
reqaction	<String>	Read-write	Name of the RADIUS action to perform if the policy matches. Minimum length = 1
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE

- UNSET
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationradiuspolicy **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationradiuspolicy":{

<b>"name":<String_value>,

</b><b>"rule":<String_value>,

</b>"reqaction":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationradiuspolicy/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationradiuspolicy **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationradiuspolicy":{

<b>"name":<String_value>,

</b>"rule":<String_value>,

"reqaction":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationradiuspolicy? **action=unset**
HTTP Method: POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationradiuspolicy":{

<b>"name":<String_value>,

</b>"rule":true,

"reqaction":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationradiuspolicy **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/authenticationradiuspolicy? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/authenticationradiuspolicy? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of authenticationradiuspolicy resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/authenticationradiuspolicy? **view=summary**

Use this query-parameter to get the summary output of authenticationradiuspolicy resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/authenticationradiuspolicy? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authenticationradiuspolicy resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationradiuspolicy": [ {

"name":<String_value>,

"rule":<String_value>,

"reqaction":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationradiuspolicy/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/ authenticationradiuspolicy/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/authenticationradiuspolicy/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of authenticationradiuspolicy resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationradiuspolicy": [ {

"name":<String_value>,

"rule":<String_value>,

"reqaction":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationradiuspolicy? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationradiuspolicy": [ { "__count": "#no"} ] }
```

authenticationradiuspolicy_authenticationvserver_binding

Binding object showing the authenticationvserver that can be bound to authenticationradiuspolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the RADIUS authentication policy. Minimum length = 1
boundto	<String>	Read-write	The entity name to which policy is bound.
priority	<Integer>	Read-only	.
activepolicy	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationradiuspolicy_authenticationvserver_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ authenticationradiuspolicy_authenticationvserver_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of authenticationradiuspolicy_authenticationvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ authenticationradiuspolicy_authenticationvserver_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authenticationradiuspolicy_authenticationvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationradiuspolicy_authenticationvserver_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"priority":<Integer_value>,

"activepolicy":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationradiuspolicy_authenticationvserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ authenticationradiuspolicy_authenticationvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationradiuspolicy_authenticationvserver_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"priority":<Integer_value>,

"activepolicy":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationradiuspolicy_authenticationvserver_binding/ name_value<String> ? **count=yes**
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"authenticationradiuspolicy_authenticationvserver_binding":
[ { "__count": "#no"} ] }
```

authenticationradiuspolicy_binding

Binding object which returns the resources bound to authenticationradiuspolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the RADIUS authentication policy. Minimum length = 1
authenticationradiuspolicy_authenticationvserver_binding	<authenticationradiuspolicy_authenticationvserver_binding[]>	Read-only	authenticationvserver that can be bound to authenticationradiuspolicy.
authenticationradiuspolicy_vpnglobal_binding	<authenticationradiuspolicy_vpnglobal_binding[]>	Read-only	vpnglobal that can be bound to authenticationradiuspolicy.
authenticationradiuspolicy_vpnvserver_binding	<authenticationradiuspolicy_vpnvserver_binding[]>	Read-only	vpnvserver that can be bound to authenticationradiuspolicy.
authenticationradiuspolicy_systemglobal_binding	<authenticationradiuspolicy_systemglobal_binding[]>	Read-only	systemglobal that can be bound to authenticationradiuspolicy.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationradiuspolicy_binding/name_value<String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationradiuspolicy_binding": [ {

"name":<String_value>,

"authenticationradiuspolicy_vpnglobal_binding":<authenticationradiuspolicy
_vpnglobal_binding[]_value>,

"authenticationradiuspolicy_authenticationvserver_binding":<authentication
radiuspolicy_authenticationvserver_binding[]_value>,

"authenticationradiuspolicy_systemglobal_binding":<authenticationradiuspol
icy_systemglobal_binding[]_value>,

"authenticationradiuspolicy_vpnvserver_binding":<authenticationradiuspolic
y_vpnvserver_binding[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationradiuspolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/authenticationradiuspolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationradiuspolicy_binding": [ {

"name":<String_value>,

"authenticationradiuspolicy_vpnglobal_binding":<authenticationradiuspolicy
_vpnglobal_binding[]_value>,

"authenticationradiuspolicy_authenticationvserver_binding":<authentication
radiuspolicy_authenticationvserver_binding[]_value>,

"authenticationradiuspolicy_systemglobal_binding":<authenticationradiuspol
icy_systemglobal_binding[]_value>,

"authenticationradiuspolicy_vpnvserver_binding":<authenticationradiuspolic
y_vpnvserver_binding[]_value>

}]}
```

authenticationradiuspolicy_systemglobal_binding

Binding object showing the systemglobal that can be bound to authenticationradiuspolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
boundto	<String>	Read-write	The entity name to which policy is bound.
name	<String>	Read-write	Name of the RADIUS authentication policy. Minimum length = 1
priority	<Integer>	Read-only	.
activepolicy	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationradiuspolicy_systemglobal_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/authenticationradiuspolicy_systemglobal_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of authenticationradiuspolicy_systemglobal_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ authenticationradiuspolicy_systemglobal_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authenticationradiuspolicy_systemglobal_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationradiuspolicy_systemglobal_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"priority":<Integer_value>,

"activepolicy":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationradiuspolicy_systemglobal_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ authenticationradiuspolicy_systemglobal_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationradiuspolicy_systemglobal_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"priority":<Integer_value>,

"activepolicy":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationradiuspolicy_systemglobal_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"authenticationradiuspolicy_systemglobal_binding": [ { "__count":
"#no"} ] }
```

authenticationradiuspolicy_vpnglobal_binding

Binding object showing the vpnglobal that can be bound to authenticationradiuspolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
boundto	<String>	Read-write	The entity name to which policy is bound.
name	<String>	Read-write	Name of the RADIUS authentication policy. Minimum length = 1
activepolicy	<Integer>	Read-only	.
priority	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of

creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationradiuspolicy_vpnglobal_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ authenticationradiuspolicy_vpnglobal_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of authenticationradiuspolicy_vpnglobal_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ authenticationradiuspolicy_vpnglobal_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authenticationradiuspolicy_vpnglobal_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationradiuspolicy_vpnglobal_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"activepolicy":<Integer_value>,

"priority":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationradiuspolicy_vpnglobal_binding
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/authenticationradiuspolicy_vpnglobal_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationradiuspolicy_vpnglobal_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"activepolicy":<Integer_value>,

"priority":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationradiuspolicy_vpnglobal_binding/name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"authenticationradiuspolicy_vpnglobal_binding": [ { "__count": "#no"} ] }
```

authenticationradiuspolicy_vpnvserver_binding

Binding object showing the vpnvserver that can be bound to authenticationradiuspolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
boundto	<String>	Read-write	The entity name to which policy is bound.
name	<String>	Read-write	Name of the RADIUS authentication policy. Minimum length = 1
activepolicy	<Integer>	Read-only	.
priority	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of

creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationradiuspolicy_vpnvserver_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ authenticationradiuspolicy_vpnvserver_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of authenticationradiuspolicy_vpnvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ authenticationradiuspolicy_vpnvserver_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authenticationradiuspolicy_vpnvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationradiuspolicy_vpnvserver_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"activepolicy":<Integer_value>,

"priority":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationradiuspolicy_vpnvserver_binding
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/authenticationradiuspolicy_vpnvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationradiuspolicy_vpnvserver_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"activepolicy":<Integer_value>,

"priority":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationradiuspolicy_vpnvserver_binding/name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"authenticationradiuspolicy_vpnvserver_binding": [ { "__count":
"#no"} ] }
```

authenticationsamlaction

Configuration for AAA Saml action resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the SAML server profile (action). Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after SAML profile is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my authentication action" or 'my

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			authentication action'). Minimum length = 1
metadataurl	<String>	Read-write	This URL is used for obtaining saml metadata. Note that it fills samlIdPCertName and samlredirectUrl fields so those fields should not be updated when metadataUrl present.
samlidpcertname	<String>	Read-write	Name of the SSL certificate used to verify responses from SAML Identity Provider (IdP). Note that if metadateURL is present then this filed should be empty. Minimum length = 1
samlsigningcertname	<String>	Read-write	Name of the SSL certificate to sign requests from ServiceProvider (SP) to Identity Provider (IdP). Minimum length = 1
samlredirecturl	<String>	Read-write	URL to which users are redirected for authentication. Note that if metadateURL is present then this

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			filed should be empty. Minimum length = 1
samlacsindex	<Integer>	Read-write	Index/ID of the metadata entry corresponding to this configuration. Default value: 255 Minimum value = 0 Maximum value = 255
samluserfield	<String>	Read-write	SAML user ID, as given in the SAML assertion. Minimum length = 1
samlrejectunsignedassertion	<String>	Read-write	Reject unsigned SAML assertions. ON option results in rejection of Assertion that is received without signature. STRICT option ensures that both Response and Assertion are signed. Default value: ON Possible values = ON, STRICT
samlissuername	<String>	Read-write	The name to be used in requests sent from Citrix ADC to IdP to uniquely identify Citrix ADC. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
samltwofactor	<String>	Read-write	Option to enable second factor after SAML. Default value: OFF Possible values = ON, OFF
preferredbindtype	<String[]>	Read-write	This element specifies the preferred binding types for sso and logout for metadata configuration. . Possible values = SSOREDIRECT, LOGOUTPOST
defaultauthentication group	<String>	Read-write	This is the default group that is chosen when the authentication succeeds in addition to extracted groups.
attribute1	<String>	Read-write	Name of the attribute in SAML Assertion whose value needs to be extracted and stored as attribute1. Maximum length of the extracted attribute is 239 bytes.
attribute2	<String>	Read-write	Name of the attribute in SAML Assertion whose value needs to be extracted and stored as attribute2. Maximum length of

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			the extracted attribute is 239 bytes.
attribute3	<String>	Read-write	Name of the attribute in SAML Assertion whose value needs to be extracted and stored as attribute3. Maximum length of the extracted attribute is 239 bytes.
attribute4	<String>	Read-write	Name of the attribute in SAML Assertion whose value needs to be extracted and stored as attribute4. Maximum length of the extracted attribute is 239 bytes.
attribute5	<String>	Read-write	Name of the attribute in SAML Assertion whose value needs to be extracted and stored as attribute5. Maximum length of the extracted attribute is 239 bytes.
attribute6	<String>	Read-write	Name of the attribute in SAML Assertion whose value needs to be extracted and stored as attribute6. Maximum length of the extracted

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			attribute is 239 bytes.
attribute7	<String>	Read-write	Name of the attribute in SAML Assertion whose value needs to be extracted and stored as attribute7. Maximum length of the extracted attribute is 239 bytes.
attribute8	<String>	Read-write	Name of the attribute in SAML Assertion whose value needs to be extracted and stored as attribute8. Maximum length of the extracted attribute is 239 bytes.
attribute9	<String>	Read-write	Name of the attribute in SAML Assertion whose value needs to be extracted and stored as attribute9. Maximum length of the extracted attribute is 239 bytes.
attribute10	<String>	Read-write	Name of the attribute in SAML Assertion whose value needs to be extracted and stored as attribute10. Maximum length of the extracted

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			attribute is 239 bytes.
attribute11	<String>	Read-write	Name of the attribute in SAML Assertion whose value needs to be extracted and stored as attribute11. Maximum length of the extracted attribute is 239 bytes.
attribute12	<String>	Read-write	Name of the attribute in SAML Assertion whose value needs to be extracted and stored as attribute12. Maximum length of the extracted attribute is 239 bytes.
attribute13	<String>	Read-write	Name of the attribute in SAML Assertion whose value needs to be extracted and stored as attribute13. Maximum length of the extracted attribute is 239 bytes.
attribute14	<String>	Read-write	Name of the attribute in SAML Assertion whose value needs to be extracted and stored as attribute14. Maximum length of the extracted

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			attribute is 239 bytes.
attribute15	<String>	Read-write	Name of the attribute in SAML Assertion whose value needs to be extracted and stored as attribute15. Maximum length of the extracted attribute is 239 bytes.
attribute16	<String>	Read-write	Name of the attribute in SAML Assertion whose value needs to be extracted and stored as attribute16. Maximum length of the extracted attribute is 239 bytes.
attributes	<String>	Read-write	List of attribute names separated by ',' which needs to be extracted. Note that preceeding and trailing spaces will be removed. Attribute name can be 127 bytes and total length of this string should not cross 2047 bytes. These attributes have multi-value

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			support separated by ',' and stored as key-value pair in AAA session.
relaystaterule	<String>	Read-write	Boolean expression that will be evaluated to validate the SAML Response. Examples: set authentication samlaction <actionname> -relaystateRule 'AAA.LOGIN.RELAYSTATE.EQ("https://fqdn.com/")' set authentication samlaction <actionname> -relaystateRule 'AAA.LOGIN.RELAYSTATE.CONTAINS("https://fqdn.com/")' set authentication samlaction <actionname> -relaystateRule 'AAA.LOGIN.RELAYSTATE.CONTAINS_ANY("patset_name")'

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			set authentication samlAction samlsp -relaystateRule 'AAA.LOGIN.RELAYSTATE.REGEX_MATCH(re#http://<regex>.com/#)'. Maximum length = 8192
signaturealg	<String>	Read-write	Algorithm to be used to sign/verify SAML transactions. Default value: RSA-SHA256 Possible values = RSA-SHA1, RSA-SHA256
digestmethod	<String>	Read-write	Algorithm to be used to compute/verify digest for SAML transactions. Default value: SHA256 Possible values = SHA1, SHA256
requestedauthncontext	<String>	Read-write	This element specifies the authentication context requirements of authentication statements returned in the response.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: exact Possible values = exact, minimum, maximum, better
authnctxclassref	<String[]>	Read-write	This element specifies the authentication class types that are requested from IdP (IdentityProvider). InternetProtocol: This is applicable when a principal is authenticated through the use of a provided IP address. InternetProtocolPassword: This is applicable when a principal is authenticated through the use of a provided IP address, in addition to a username/ password. Kerberos: This is applicable when the principal has authenticated using a password to a local authentication authority, in order to

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			acquire a Kerberos ticket. MobileOneFactorUnregistered: This indicates authentication of the mobile device without requiring explicit end-user interaction. MobileTwoFactorUnregistered: This indicates two-factor based authentication during mobile customer registration process, such as secure device and user PIN. MobileOneFactorContract: Reflects mobile contract customer registration procedures and a single factor authentication. MobileTwoFactorContract: Reflects mobile contract customer

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			registration procedures and a two-factor based authentication. Password: This class is applicable when a principal authenticates using password over unprotected http session. PasswordProtected Transport: This class is applicable when a principal authenticates to an authentication authority through the presentation of a password over a protected session. PreviousSession: This class is applicable when a principal had authenticated to an authentication authority at some point in the past using any authentication context.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			X509: This indicates that the principal authenticated by means of a digital signature where the key was validated as part of an X.509 Public Key Infrastructure. PGP: This indicates that the principal authenticated by means of a digital signature where the key was validated as part of a PGP Public Key Infrastructure. SPKI: This indicates that the principal authenticated by means of a digital signature where the key was validated via an SPKI Infrastructure. XMLDSig: This indicates that the principal authenticated by means of a digital signature according to the processing rules specified in

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			the XML Digital Signature specification. Smartcard: This indicates that the principal has authenticated using smartcard. SmartcardPKI: This class is applicable when a principal authenticates to an authentication authority through a two-factor authentication mechanism using a smartcard with enclosed private key and a PIN. SoftwarePKI: This class is applicable when a principal uses an X.509 certificate stored in software to authenticate to the authentication authority. Telephony: This class is used to indicate that the principal

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			authenticated via the provision of a fixed-line telephone number, transported via a telephony protocol such as ADSL. NomadTelephony: Indicates that the principal is "roaming" and authenticates via the means of the line number, a user suffix, and a password element. PersonalTelephony: This class is used to indicate that the principal authenticated via the provision of a fixed-line telephone. AuthenticatedTelephony: Indicates that the principal authenticated via the means of the line number, a user suffix, and a password element.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			SecureRemotePassword: This class is applicable when the authentication was performed by means of Secure Remote Password. TLSClient: This class indicates that the principal authenticated by means of a client certificate, secured with the SSL/TLS transport. TimeSyncToken: This is applicable when a principal authenticates through a time synchronization token. Unspecified: This indicates that the authentication was performed by unspecified means. Windows: This indicates that Windows integrated authentication is

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			utilized for authentication. Possible values = InternetProtocol, InternetProtocolPassword, Kerberos, MobileOneFactorUnregistered, MobileTwoFactorUnregistered, MobileOneFactorContract, MobileTwoFactorContract, Password, PasswordProtectedTransport, PreviousSession, X509, PGP, SPKI, XMLDSig, Smartcard, SmartcardPKI, SoftwarePKI, Telephony, NomadTelephony, PersonalTelephony, AuthenticatedTelephony, SecureRemotePassword, TLSClient, TimeSyncToken, Unspecified, Windows
customauthnctxclassref	<String>	Read-write	This element specifies the custom authentication class

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			reference to be sent as a part of the Authentication Request that is sent by the SP to SAML IDP. The input string must be the body of the authentication class being requested. Input format: Alphanumeric string or URL specifying the body of the Request.If more than one string has to be provided, then the same can be done by specifying the classes as a string of comma separated values. Example input: set authentication samlaction samlact1 -customAuthnCtxClassRef http://www.class1.com/LoA1,http://www.class2.com/LoA2 . Maximum length = 512

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
samlbinding	<String>	Read-write	This element specifies the transport mechanism of saml messages. Default value: POST Possible values = REDIRECT, POST, ARTIFACT
attributeconsumingserviceindex	<Integer>	Read-write	Index/ID of the attribute specification at Identity Provider (IdP). IdP will locate attributes requested by SP using this index and send those attributes in Assertion. Default value: 255 Minimum value = 0 Maximum value = 255
sendthumbprint	<String>	Read-write	Option to send thumbprint instead of x509 certificate in SAML request. Default value: OFF Possible values = ON, OFF
enforceusername	<String>	Read-write	Option to choose whether the username that is extracted from SAML assertion can be

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			edited in login page while doing second factor. Default value: ON Possible values = ON, OFF
logouturl	<String>	Read-write	SingleLogout URL on IdP to which logoutRequest will be sent on Citrix ADC session cleanup.
artifactresolutionservi ceurl	<String>	Read-write	URL of the Artifact Resolution Service on IdP to which Citrix ADC will post artifact to get actual SAML token.
skewtime	<Integer>	Read-write	This option specifies the allowed clock skew in number of minutes that Citrix ADC ServiceProvider allows on an incoming assertion. For example, if skewTime is 10, then assertion would be valid from (current time - 10) min to (current time + 10) min, ie 20min in all. Default value: 5
logoutbinding	<String>	Read-write	This element specifies the transport mechanism

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			of saml logout messages. Default value: POST Possible values = REDIRECT, POST
forceauthn	<String>	Read-write	Option that forces authentication at the Identity Provider (IdP) that receives Citrix ADC's request. Default value: OFF Possible values = ON, OFF
groupnamefield	<String>	Read-write	Name of the tag in assertion that contains user groups.
audience	<String>	Read-write	Audience for which assertion sent by IdP is applicable. This is typically entity name or url that represents ServiceProvider.
metadatarefreshinterval	<Integer>	Read-write	Interval in minutes for fetching metadata from specified metadata URL. Default value: 3600
storesamlresponse	<String>	Read-write	Option to store entire SAML Response through the life of user session.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: OFF Possible values = ON, OFF
statechecks	<String>	Read-write	Boolean expression that will be evaluated to validate HTTP requests on SAML endpoints. Examples: set authentication samlaction <actionname> -stateChecks 'HTTP.REQ.HOSTNAME.EQ("https://fqdn.com/")' . Maximum length = 8191
metadataimportstatus	<String>	Read-only	Describes metadata import status. Default value: SUCCESS Possible values = INIT, SUCCESS, FAIL
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationsamlaction **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationsamlaction":{

<b>"name":<String_value>,

</b>"metadataurl":<String_value>,

"samlidpcertname":<String_value>,

"samlsigningcertname":<String_value>,

"samlredirecturl":<String_value>,

"samlacsindex":<Integer_value>,

"samluserfield":<String_value>,

"samlrejectunsignedassertion":<String_value>,

"samlissuername":<String_value>,

"samltwofactor":<String_value>,

"preferredbindtype":<String[]_value>,

"defaultauthenticationgroup":<String_value>,

"attribute1":<String_value>,

"attribute2":<String_value>,

"attribute3":<String_value>,

"attribute4":<String_value>,

"attribute5":<String_value>,

"attribute6":<String_value>,
```

```
"attribute7":<String_value>,

"attribute8":<String_value>,

"attribute9":<String_value>,

"attribute10":<String_value>,

"attribute11":<String_value>,

"attribute12":<String_value>,

"attribute13":<String_value>,

"attribute14":<String_value>,

"attribute15":<String_value>,

"attribute16":<String_value>,

"attributes":<String_value>,

"relaystaterule":<String_value>,

"signaturealg":<String_value>,

"digestmethod":<String_value>,

"requestedauthncontext":<String_value>,

"authnctxclassref":<String[]_value>,

"customauthnctxclassref":<String_value>,

"samlbinding":<String_value>,

"attributeconsumingserviceindex":<Integer_value>,

"sendthumbprint":<String_value>,

"enforceusername":<String_value>,

"logouturl":<String_value>,
```

```
"artifactresolutionserviceurl":<String_value>,

"skewtime":<Integer_value>,

"logoutbinding":<String_value>,

"forceauthn":<String_value>,

"groupnamefield":<String_value>,

"audience":<String_value>,

"metadatarefreshinterval":<Integer_value>,

"storesamlresponse":<String_value>,

"statechecks":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationsamlaction/ name_value<String>
HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationsamlaction **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationsamlaction":{

<b>"name":<String_value>,

</b>"metadataurl":<String_value>,

"samlidpcertname":<String_value>,

"samlsigningcertname":<String_value>,

"samlredirecturl":<String_value>,

"samlacsindex":<Integer_value>,

"samluserfield":<String_value>,

"samlrejectunsignedassertion":<String_value>,

"samlissuername":<String_value>,

"samltwofactor":<String_value>,

"preferredbindtype":<String[]_value>,

"defaultauthenticationgroup":<String_value>,

"attribute1":<String_value>,

"attribute2":<String_value>,

"attribute3":<String_value>,

"attribute4":<String_value>,

"attribute5":<String_value>,

"attribute6":<String_value>,
```

```
"attribute7":<String_value>,

"attribute8":<String_value>,

"attribute9":<String_value>,

"attribute10":<String_value>,

"attribute11":<String_value>,

"attribute12":<String_value>,

"attribute13":<String_value>,

"attribute14":<String_value>,

"attribute15":<String_value>,

"attribute16":<String_value>,

"attributes":<String_value>,

"relaystaterule":<String_value>,

"signaturealg":<String_value>,

"digestmethod":<String_value>,

"requestedauthncontext":<String_value>,

"authnctxclassref":<String[]_value>,

"customauthnctxclassref":<String_value>,

"samlbinding":<String_value>,

"attributeconsumingserviceindex":<Integer_value>,

"sendthumbprint":<String_value>,

"enforceusername":<String_value>,

"logouturl":<String_value>,
```

```
"artifactresolutionserviceurl":<String_value>,

"skewtime":<Integer_value>,

"logoutbinding":<String_value>,

"forceauthn":<String_value>,

"groupnamefield":<String_value>,

"audience":<String_value>,

"metadatarefreshinterval":<Integer_value>,

"storesamlresponse":<String_value>,

"statechecks":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationsamlaction? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationsamlaction":{

<b>"name":<String_value>,
```

```
</b>"metadataurl":true,

"samlsigningcertname":true,

"samlredirecturl":true,

"samlacsindex":true,

"samluserfield":true,

"samlrejectunsignedassertion":true,

"samlissuername":true,

"samltwofactor":true,

"preferredbindtype":true,

"defaultauthenticationgroup":true,

"attribute1":true,

"attribute2":true,

"attribute3":true,

"attribute4":true,

"attribute5":true,

"attribute6":true,

"attribute7":true,

"attribute8":true,

"attribute9":true,

"attribute10":true,

"attribute11":true,

"attribute12":true,
```

```
"attribute13":true,
"attribute14":true,
"attribute15":true,
"attribute16":true,
"attributes":true,
"relaystaterule":true,
"signaturealg":true,
"digestmethod":true,
"requestedauthncontext":true,
"authnctxclassref":true,
"customauthnctxclassref":true,
"samlbinding":true,
"attributeconsumingserviceindex":true,
"sendthumbprint":true,
"enforceusername":true,
"logouturl":true,
"artifactresolutionserviceurl":true,
"skewtime":true,
"logoutbinding":true,
"forceauthn":true,
"groupnamefield":true,
"audience":true,
```

```
"metadatarefreshinterval":true,

"storesamlresponse":true,

"statechecks":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationsamlaction **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/authenticationsamlaction? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/authenticationsamlaction? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of authenticationsamlaction resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/authenticationsamlaction? **view=summary**

Use this query-parameter to get the summary output of authenticationsamlaction resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/authenticationsamlaction? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authenticationsamlaction resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationsamlaction": [ {

"name":<String_value>,

"metadataurl":<String_value>,

"preferredbindtype":<String[]_value>,

"samlidpcertname":<String_value>,

"samlsigningcertname":<String_value>,

"samlredirecturl":<String_value>,

"samlacsindex":<Integer_value>,

"samluserfield":<String_value>,

"samlrejectunsignedassertion":<String_value>,

"samlissuername":<String_value>,

"samltwofactor":<String_value>,

"defaultauthenticationgroup":<String_value>,

"attribute1":<String_value>,

"attribute2":<String_value>,
```

```
"attribute3":<String_value>,

"attribute4":<String_value>,

"attribute5":<String_value>,

"attribute6":<String_value>,

"attribute7":<String_value>,

"attribute8":<String_value>,

"attribute9":<String_value>,

"attribute10":<String_value>,

"attribute11":<String_value>,

"attribute12":<String_value>,

"attribute13":<String_value>,

"attribute14":<String_value>,

"attribute15":<String_value>,

"attribute16":<String_value>,

"attributes":<String_value>,

"relaystaterule":<String_value>,

"signaturealg":<String_value>,

"digestmethod":<String_value>,

"requestedauthncontext":<String_value>,

"authnctxclassref":<String[]_value>,

"customauthnctxclassref":<String_value>,

"samlbinding":<String_value>,
```

```
"attributeconsumingserviceindex":<Integer_value>,

"sendthumbprint":<String_value>,

"enforceusername":<String_value>,

"logouturl":<String_value>,

"artifactresolutionserviceurl":<String_value>,

"skewtime":<Integer_value>,

"logoutbinding":<String_value>,

"forceauthn":<String_value>,

"groupnamefield":<String_value>,

"audience":<String_value>,

"metadatarefreshinterval":<Integer_value>,

"metadataimportstatus":<String_value>,

"storesamlresponse":<String_value>,

"statechecks":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationsamlaction/ name_value<String>
Query-parameters: attrs http:// <netscaler-ip-address> /nitro/v1/config/authenticationsamlaction/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/authenticationsamlaction/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of authenticationsamlaction resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationsamlaction": [ {

"name":<String_value>,

"metadataurl":<String_value>,

"preferredbindtype":<String[]_value>,

"samlidpcertname":<String_value>,

"samlsigningcertname":<String_value>,

"samlredirecturl":<String_value>,

"samlacsindex":<Integer_value>,

"samluserfield":<String_value>,

"samlrejectunsignedassertion":<String_value>,
```

```
"samlissuername":<String_value>,

"samltwofactor":<String_value>,

"defaultauthenticationgroup":<String_value>,

"attribute1":<String_value>,

"attribute2":<String_value>,

"attribute3":<String_value>,

"attribute4":<String_value>,

"attribute5":<String_value>,

"attribute6":<String_value>,

"attribute7":<String_value>,

"attribute8":<String_value>,

"attribute9":<String_value>,

"attribute10":<String_value>,

"attribute11":<String_value>,

"attribute12":<String_value>,

"attribute13":<String_value>,

"attribute14":<String_value>,

"attribute15":<String_value>,

"attribute16":<String_value>,

"attributes":<String_value>,

"relaystaterule":<String_value>,

"signaturealg":<String_value>,
```

```
"digestmethod":<String_value>,

"requestedauthncontext":<String_value>,

"authnctxclassref":<String[]_value>,

"customauthnctxclassref":<String_value>,

"samlbinding":<String_value>,

"attributeconsumingserviceindex":<Integer_value>,

"sendthumbprint":<String_value>,

"enforceusername":<String_value>,

"logouturl":<String_value>,

"artifactresolutionserviceurl":<String_value>,

"skewtime":<Integer_value>,

"logoutbinding":<String_value>,

"forceauthn":<String_value>,

"groupnamefield":<String_value>,

"audience":<String_value>,

"metadatarefreshinterval":<Integer_value>,

"metadataimportstatus":<String_value>,

"storesamlresponse":<String_value>,

"statechecks":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

```
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationsamlaction? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationsamlaction": [ { "__count": "#no"} ] }
```

authenticationsamlidppolicy

Configuration for AAA Saml IdentityProvider (IdP) policy resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the SAML Identity Provider (IdP) authentication policy. This is used for configuring Citrix ADC as SAML Identity Provider. Must begin with an

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the policy is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my policy" or 'my policy'). Minimum length = 1
rule	<String>	Read-write	Expression which is evaluated to choose a profile for authentication. The following requirements apply only to the Citrix ADC CLI:

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			* If the expression includes one or more spaces, enclose the entire expression in double quotation marks. * If the expression itself includes double quotation marks, escape the quotations by using the \ character. * Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks. Minimum length = 1
action	<String>	Read-write	Name of the profile to apply to requests or connections that match this policy. Minimum length = 1
undefaction	<String>	Read-write	Action to perform if the result of policy evaluation is undefined (UNDEF). An UNDEF event indicates an internal error condition. Only

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			the above built-in actions can be used.
comment	<String>	Read-write	Any comments to preserve information about this policy.
logaction	<String>	Read-write	Name of messagelog action to use when a request matches this policy.
newname	<String>	Read-write	New name for the SAML IdentityProvider policy. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space ( ), at (@), equals (=), colon (:), and underscore characters. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			marks (for example, "my samlidppolicy policy" or 'my samlidppolicy policy'). Minimum length = 1
gotopriorityexpression	<String>	Read-only	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
hits	<Integer>	Read-only	Number of hits.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT
- RENAME

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationsamlidppolicy **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationsamlidppolicy":{

<b>"name":<String_value>,

</b><b>"rule":<String_value>,
```

```
</b><b>"action":<String_value>,

</b>"undefaction":<String_value>,

"comment":<String_value>,

"logaction":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationsamlidppolicy/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationsamlidppolicy **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationsamlidppolicy":{

<b>"name":<String_value>,

</b>"rule":<String_value>,

"action":<String_value>,

"undefaction":<String_value>,

"comment":<String_value>,

"logaction":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationsamlidppolicy? **action=unset**
HTTP Method: POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationsamlidppolicy":{

<b>"name":<String_value>,

</b>"undefaction":true,

"comment":true,

"logaction":true
```

```
}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

RENAME

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationsamlidppolicy? **action=rename**
HTTP Method: POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationsamlidppolicy":{

<b>"name":<String_value>,

</b><b>"newname":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationsamlidppolicy **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/authenticationsamlidppolicy? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/authenticationsamlidppolicy? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of authenticationsamlidppolicy resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/authenticationsamlidppolicy? **view=summary**

Use this query-parameter to get the summary output of authenticationsamlidppolicy resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/authenticationsamlidppolicy? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authenticationsamlidppolicy resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationsamlidppolicy": [ {

"name":<String_value>,

"rule":<String_value>,

"action":<String_value>,
```

```
"undefaction":<String_value>,

"comment":<String_value>,

"logaction":<String_value>,

"gotopriorityexpression":<String_value>,

"hits":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationsamlidppolicy/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/ authenticationsamlidppolicy/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/authenticationsamlidppolicy/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of authenticationsamlidppolicy resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationsamlidppolicy": [ {

"name":<String_value>,

"rule":<String_value>,

"action":<String_value>,

"undefaction":<String_value>,

"comment":<String_value>,

"logaction":<String_value>,

"gotopriorityexpression":<String_value>,

"hits":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationsamlidppolicy? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationsamlidppolicy": [ { "__count": "#no"} ] }
```

authenticationsamlidppolicy_authenticationvserver_binding

Binding object showing the authenticationvserver that can be bound to authenticationsamlidppolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
boundto	<String>	Read-write	The entity name to which policy is bound.
name	<String>	Read-write	Name of the SAML IdentityProvider (IdP) policy for which to display detailed information. Minimum length = 1
activepolicy	<Integer>	Read-only	.
priority	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationsamlidppolicy_authenticationvserver_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/authenticationsamlidppolicy_authenticationvserver_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of authenticationsamlidppolicy_authenticationvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/authenticationsamlidppolicy_authenticationvserver_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authenticationsamlidppolicy_authenticationvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationsamlidppolicy_authenticationvserver_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"activepolicy":<Integer_value>,

"priority":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationsamlidppolicy_authenticationvserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ authenticationsamlidppolicy_authenticationvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationsamlidppolicy_authenticationvserver_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"activepolicy":<Integer_value>,

"priority":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationsamlidppolicy_authenticationvserver_binding/ name_value<String> ? **count=yes**
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"authenticationsamlidppolicy_authenticationvserver_binding":
[ { "__count": "#no"} ] }
```

authenticationsamlidppolicy_binding

Binding object which returns the resources bound to authenticationsamlidppolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the SAML IdentityProvider (IdP) policy for which to display detailed information. Minimum length = 1
authenticationsamlidppolicy_authenticationvserver_binding	<authenticationsamlidppolicy_authenticationvserver_binding[]>	Read-only	authenticationvserver that can be bound to authenticationsamlidppolicy.
authenticationsamlidppolicy_vpnvserver_binding	<authenticationsamlidppolicy_vpnvserver_binding[]>	Read-only	vpnvserver that can be bound to authenticationsamlidppolicy.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationsamlidppolicy_binding/name_value<String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationsamlidppolicy_binding": [ {

"name":<String_value>,

"authenticationsamlidppolicy_authenticationvserver_binding":<authenticatio
nsamlidppolicy_authenticationvserver_binding[]_value>,

"authenticationsamlidppolicy_vpnvserver_binding":<authenticationsamlidppol
icy_vpnvserver_binding[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationsamlidppolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/authenticationsamlidppolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationsamlidppolicy_binding": [ {

"name":<String_value>,

"authenticationsamlidppolicy_authenticationvserver_binding":<authenticatio
nsamlidppolicy_authenticationvserver_binding[]_value>,

"authenticationsamlidppolicy_vpnvserver_binding":<authenticationsamlidppol
icy_vpnvserver_binding[]_value>

}]}
```

authenticationsamlidppolicy_vpnvserver_binding

Binding object showing the vpnvserver that can be bound to authenticationsamlidppolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
boundto	<String>	Read-write	The entity name to which policy is bound.
name	<String>	Read-write	Name of the SAML IdentityProvider (IdP) policy for which to display detailed information. Minimum length = 1
activepolicy	<Integer>	Read-only	.
priority	<Integer>	Read-only	.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationsamlidppolicy_vpnvserver_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/authenticationsamlidppolicy_vpnvserver_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of authenticationsamlidppolicy_vpnvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ authenticationsamlidppolicy_vpnvserver_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authenticationsamlidppolicy_vpnvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationsamlidppolicy_vpnvserver_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"activepolicy":<Integer_value>,
```

```
"priority":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationsamlidppolicy_vpnvserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ authenticationsamlidppolicy_vpnvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationsamlidppolicy_vpnvserver_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"activepolicy":<Integer_value>,

"priority":<Integer_value>
```

```
}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationsamlidppolicy_vpnvserver_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"authenticationsamlidppolicy_vpnvserver_binding": [ { "__count":
"#no"} ] }
```

authenticationsamlidpprofile

Configuration for AAA Saml IdentityProvider (IdP) profile resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the new saml single sign-on profile. Must begin with an ASCII

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after an action is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my action" or 'my action'). Minimum length = 1
samlspcertname	<String>	Read-write	Name of the SSL certificate of SAML Relying Party. This certificate is used to verify signature of the incoming AuthnRequest from a Relying Party or Service Provider. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
samlidpcertname	<String>	Read-write	Name of the certificate used to sign the SAMLResposne that is sent to Relying Party or Service Provider after successful authentication. Minimum length = 1
assertionconsumerserviceurl	<String>	Read-write	URL to which the assertion is to be sent. Minimum length = 1
sendpassword	<String>	Read-write	Option to send password in assertion. Default value: OFF Possible values = ON, OFF
samlissuername	<String>	Read-write	The name to be used in requests sent from Citrix ADC to IdP to uniquely identify Citrix ADC. Minimum length = 1
rejectunsignedrequests	<String>	Read-write	Option to Reject unsigned SAML Requests. ON option denies any authentication requests that arrive without signature. Default value: ON

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ON, OFF
signaturealg	<String>	Read-write	Algorithm to be used to sign/verify SAML transactions. Default value: RSA-SHA256 Possible values = RSA-SHA1, RSA-SHA256
digestmethod	<String>	Read-write	Algorithm to be used to compute/verify digest for SAML transactions. Default value: SHA256 Possible values = SHA1, SHA256
audience	<String>	Read-write	Audience for which assertion sent by IdP is applicable. This is typically entity name or url that represents ServiceProvider.
nameidformat	<String>	Read-write	Format of Name Identifier sent in Assertion. Default value: transient Possible values = Unspecified, emailAddress, X509SubjectName,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			WindowsDomainQualifiedName, kerberos, entity, persistent, transient
nameidexpr	<String>	Read-write	Expression that will be evaluated to obtain NameIdentifier to be sent in assertion. Maximum length = 128
attribute1	<String>	Read-write	Name of attribute1 that needs to be sent in SAML Assertion.
attribute1expr	<String>	Read-write	Expression that will be evaluated to obtain attribute1's value to be sent in Assertion. Maximum length = 128
attribute1friendlyname	<String>	Read-write	User-Friendly Name of attribute1 that needs to be sent in SAML Assertion.
attribute1format	<String>	Read-write	Format of Attribute1 to be sent in Assertion. Possible values = URI, Basic
attribute2	<String>	Read-write	Name of attribute2 that needs to be sent in SAML Assertion.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
attribute2expr	<String>	Read-write	Expression that will be evaluated to obtain attribute2's value to be sent in Assertion. Maximum length = 128
attribute2friendlyname	<String>	Read-write	User-Friendly Name of attribute2 that needs to be sent in SAML Assertion.
attribute2format	<String>	Read-write	Format of Attribute2 to be sent in Assertion. Possible values = URI, Basic
attribute3	<String>	Read-write	Name of attribute3 that needs to be sent in SAML Assertion.
attribute3expr	<String>	Read-write	Expression that will be evaluated to obtain attribute3's value to be sent in Assertion. Maximum length = 128
attribute3friendlyname	<String>	Read-write	User-Friendly Name of attribute3 that needs to be sent in SAML Assertion.
attribute3format	<String>	Read-write	Format of Attribute3 to be sent in Assertion.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = URI, Basic
attribute4	<String>	Read-write	Name of attribute4 that needs to be sent in SAML Assertion.
attribute4expr	<String>	Read-write	Expression that will be evaluated to obtain attribute4's value to be sent in Assertion. Maximum length = 128
attribute4friendlyname	<String>	Read-write	User-Friendly Name of attribute4 that needs to be sent in SAML Assertion.
attribute4format	<String>	Read-write	Format of Attribute4 to be sent in Assertion. Possible values = URI, Basic
attribute5	<String>	Read-write	Name of attribute5 that needs to be sent in SAML Assertion.
attribute5expr	<String>	Read-write	Expression that will be evaluated to obtain attribute5's value to be sent in Assertion. Maximum length = 128
attribute5friendlyname	<String>	Read-write	User-Friendly Name of attribute5 that

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			needs to be sent in SAML Assertion.
attribute5format	<String>	Read-write	Format of Attribute5 to be sent in Assertion. Possible values = URI, Basic
attribute6	<String>	Read-write	Name of attribute6 that needs to be sent in SAML Assertion.
attribute6expr	<String>	Read-write	Expression that will be evaluated to obtain attribute6's value to be sent in Assertion. Maximum length = 128
attribute6friendlyname	<String>	Read-write	User-Friendly Name of attribute6 that needs to be sent in SAML Assertion.
attribute6format	<String>	Read-write	Format of Attribute6 to be sent in Assertion. Possible values = URI, Basic
attribute7	<String>	Read-write	Name of attribute7 that needs to be sent in SAML Assertion.
attribute7expr	<String>	Read-write	Expression that will be evaluated to obtain attribute7's

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			value to be sent in Assertion. Maximum length = 128
attribute7friendlyname	<String>	Read-write	User-Friendly Name of attribute7 that needs to be sent in SAML Assertion.
attribute7format	<String>	Read-write	Format of Attribute7 to be sent in Assertion. Possible values = URI, Basic
attribute8	<String>	Read-write	Name of attribute8 that needs to be sent in SAML Assertion.
attribute8expr	<String>	Read-write	Expression that will be evaluated to obtain attribute8's value to be sent in Assertion. Maximum length = 128
attribute8friendlyname	<String>	Read-write	User-Friendly Name of attribute8 that needs to be sent in SAML Assertion.
attribute8format	<String>	Read-write	Format of Attribute8 to be sent in Assertion. Possible values = URI, Basic

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
attribute9	<String>	Read-write	Name of attribute9 that needs to be sent in SAML Assertion.
attribute9expr	<String>	Read-write	Expression that will be evaluated to obtain attribute9's value to be sent in Assertion. Maximum length = 128
attribute9friendlyname	<String>	Read-write	User-Friendly Name of attribute9 that needs to be sent in SAML Assertion.
attribute9format	<String>	Read-write	Format of Attribute9 to be sent in Assertion. Possible values = URI, Basic
attribute10	<String>	Read-write	Name of attribute10 that needs to be sent in SAML Assertion.
attribute10expr	<String>	Read-write	Expression that will be evaluated to obtain attribute10's value to be sent in Assertion. Maximum length = 128
attribute10friendlyname	<String>	Read-write	User-Friendly Name of attribute10 that needs to be sent in SAML Assertion.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
attribute10format	<String>	Read-write	Format of Attribute10 to be sent in Assertion. Possible values = URI, Basic
attribute11	<String>	Read-write	Name of attribute11 that needs to be sent in SAML Assertion.
attribute11expr	<String>	Read-write	Expression that will be evaluated to obtain attribute11's value to be sent in Assertion. Maximum length = 128
attribute11friendlyname	<String>	Read-write	User-Friendly Name of attribute11 that needs to be sent in SAML Assertion.
attribute11format	<String>	Read-write	Format of Attribute11 to be sent in Assertion. Possible values = URI, Basic
attribute12	<String>	Read-write	Name of attribute12 that needs to be sent in SAML Assertion.
attribute12expr	<String>	Read-write	Expression that will be evaluated to obtain attribute12's value to be sent in Assertion. Maximum length = 128

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
attribute12friendlyname	<String>	Read-write	User-Friendly Name of attribute12 that needs to be sent in SAML Assertion.
attribute12format	<String>	Read-write	Format of Attribute12 to be sent in Assertion. Possible values = URI, Basic
attribute13	<String>	Read-write	Name of attribute13 that needs to be sent in SAML Assertion.
attribute13expr	<String>	Read-write	Expression that will be evaluated to obtain attribute13's value to be sent in Assertion. Maximum length = 128
attribute13friendlyname	<String>	Read-write	User-Friendly Name of attribute13 that needs to be sent in SAML Assertion.
attribute13format	<String>	Read-write	Format of Attribute13 to be sent in Assertion. Possible values = URI, Basic
attribute14	<String>	Read-write	Name of attribute14 that needs to be sent in SAML Assertion.
attribute14expr	<String>	Read-write	Expression that will be evaluated to

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			obtain attribute14's value to be sent in Assertion. Maximum length = 128
attribute14friendlyname	<String>	Read-write	User-Friendly Name of attribute14 that needs to be sent in SAML Assertion.
attribute14format	<String>	Read-write	Format of Attribute14 to be sent in Assertion. Possible values = URI, Basic
attribute15	<String>	Read-write	Name of attribute15 that needs to be sent in SAML Assertion.
attribute15expr	<String>	Read-write	Expression that will be evaluated to obtain attribute15's value to be sent in Assertion. Maximum length = 128
attribute15friendlyname	<String>	Read-write	User-Friendly Name of attribute15 that needs to be sent in SAML Assertion.
attribute15format	<String>	Read-write	Format of Attribute15 to be sent in Assertion. Possible values = URI, Basic

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
attribute16	<String>	Read-write	Name of attribute16 that needs to be sent in SAML Assertion.
attribute16expr	<String>	Read-write	Expression that will be evaluated to obtain attribute16's value to be sent in Assertion. Maximum length = 128
attribute16friendlyname	<String>	Read-write	User-Friendly Name of attribute16 that needs to be sent in SAML Assertion.
attribute16format	<String>	Read-write	Format of Attribute16 to be sent in Assertion. Possible values = URI, Basic
encryptassertion	<String>	Read-write	Option to encrypt assertion when Citrix ADC IDP sends one. Default value: OFF Possible values = ON, OFF
encryptionalgorithm	<String>	Read-write	Algorithm to be used to encrypt SAML assertion. Default value: AES256 Possible values = DES3, AES128, AES192, AES256

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
samlbinding	<String>	Read-write	This element specifies the transport mechanism of saml messages. Default value: POST Possible values = REDIRECT, POST, ARTIFACT
skewtime	<Integer>	Read-write	This option specifies the number of minutes on either side of current time that the assertion would be valid. For example, if skewTime is 10, then assertion would be valid from (current time - 10) min to (current time + 10) min, ie 20min in all. Default value: 5
serviceproviderid	<String>	Read-write	Unique identifier of the Service Provider that sends SAML Request. Citrix ADC will ensure that the Issuer of the SAML Request matches this URI. In case of SP initiated sign-in scenarios, this value must be same as samlIssuerName configured in samlAction.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum length = 1
signassertion	<String>	Read-write	Option to sign portions of assertion when Citrix ADC IDP sends one. Based on the user selection, either Assertion or Response or Both or none can be signed. Default value: ASSERTION Possible values = NONE, ASSERTION, RESPONSE, BOTH
keytransportalg	<String>	Read-write	Key transport algorithm to be used in encryption of SAML assertion. Default value: RSA_OAEP Possible values = RSA-V1_5, RSA_OAEP
splogouturl	<String>	Read-write	Endpoint on the ServiceProvider (SP) to which logout messages are to be sent. Minimum length = 1
logoutbinding	<String>	Read-write	This element specifies the transport mechanism

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			of saml logout messages. Default value: POST Possible values = REDIRECT, POST
defaultauthenticationgroup	<String>	Read-write	This group will be part of AAA session's internal group list. This will be helpful to admin in Nfactor flow to decide right AAA configuration for Relaying Party. In authentication policy AAA.USER.IS_MEMBER_OF("<default_auth_group>") is way to use this feature.
metadataurl	<String>	Read-write	This URL is used for obtaining samlidp metadata.
metadatarefreshinterval	<Integer>	Read-write	Interval in minute for fetching metadata from specified metadata URL. Default value: 3600
signatureservice	<String>	Read-write	Name of the service in cloud used to sign the data. Minimum length = 1
samlsigningcertversion	<String>	Read-write	version of the certificate in signature service used to sign the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			SAMLResposne that is sent to Relying Party or Service Provider after successful authentication. Minimum length = 1
samlspcertversion	<String>	Read-write	version of the certificate in signature service used to verify the signature of the incoming AuthnRequest from a Relying Party or Service Provider. Minimum length = 1
acsurlrule	<String>	Read-write	Expression that will be evaluated to allow Assertion Consumer Service URI coming in the SAML Request. Maximum length = 8191
metadataimportstatus	<String>	Read-only	Describes metadata import status. Default value: INIT Possible values = INIT, SUCCESS, FAIL
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationsamlidpprofile **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationsamlidpprofile":{

<b>"name":<String_value>,

</b>"samlspcertname":<String_value>,

"samlidpcertname":<String_value>,

"assertionconsumerserviceurl":<String_value>,

"sendpassword":<String_value>,

"samlissuername":<String_value>,

"rejectunsignedrequests":<String_value>,

"signaturealg":<String_value>,

"digestmethod":<String_value>,

"audience":<String_value>,

"nameidformat":<String_value>,

"nameidexpr":<String_value>,

"attribute1":<String_value>,

"attribute1expr":<String_value>,

"attribute1friendlyname":<String_value>,
```

```
"attribute1format":<String_value>,

"attribute2":<String_value>,

"attribute2expr":<String_value>,

"attribute2friendlyname":<String_value>,

"attribute2format":<String_value>,

"attribute3":<String_value>,

"attribute3expr":<String_value>,

"attribute3friendlyname":<String_value>,

"attribute3format":<String_value>,

"attribute4":<String_value>,

"attribute4expr":<String_value>,

"attribute4friendlyname":<String_value>,

"attribute4format":<String_value>,

"attribute5":<String_value>,

"attribute5expr":<String_value>,

"attribute5friendlyname":<String_value>,

"attribute5format":<String_value>,

"attribute6":<String_value>,

"attribute6expr":<String_value>,

"attribute6friendlyname":<String_value>,

"attribute6format":<String_value>,

"attribute7":<String_value>,
```

```
"attribute7expr":<String_value>,

"attribute7friendlyname":<String_value>,

"attribute7format":<String_value>,

"attribute8":<String_value>,

"attribute8expr":<String_value>,

"attribute8friendlyname":<String_value>,

"attribute8format":<String_value>,

"attribute9":<String_value>,

"attribute9expr":<String_value>,

"attribute9friendlyname":<String_value>,

"attribute9format":<String_value>,

"attribute10":<String_value>,

"attribute10expr":<String_value>,

"attribute10friendlyname":<String_value>,

"attribute10format":<String_value>,

"attribute11":<String_value>,

"attribute11expr":<String_value>,

"attribute11friendlyname":<String_value>,

"attribute11format":<String_value>,

"attribute12":<String_value>,

"attribute12expr":<String_value>,

"attribute12friendlyname":<String_value>,
```

```
"attribute12format":<String_value>,

"attribute13":<String_value>,

"attribute13expr":<String_value>,

"attribute13friendlyname":<String_value>,

"attribute13format":<String_value>,

"attribute14":<String_value>,

"attribute14expr":<String_value>,

"attribute14friendlyname":<String_value>,

"attribute14format":<String_value>,

"attribute15":<String_value>,

"attribute15expr":<String_value>,

"attribute15friendlyname":<String_value>,

"attribute15format":<String_value>,

"attribute16":<String_value>,

"attribute16expr":<String_value>,

"attribute16friendlyname":<String_value>,

"attribute16format":<String_value>,

"encryptassertion":<String_value>,

"encryptionalgorithm":<String_value>,

"samlbinding":<String_value>,

"skewtime":<Integer_value>,

"serviceproviderid":<String_value>,
```

```
"signassertion":<String_value>,

"keytransportalg":<String_value>,

"splogouturl":<String_value>,

"logoutbinding":<String_value>,

"defaultauthenticationgroup":<String_value>,

"metadataurl":<String_value>,

"metadatarefreshinterval":<Integer_value>,

"signatureservice":<String_value>,

"samlsigningcertversion":<String_value>,

"samlspcertversion":<String_value>,

"acsurlrule":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationsamlidpprofile/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationsamlidpprofile **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationsamlidpprofile":{

<b>"name":<String_value>,

</b>"samlspcertname":<String_value>,

"samlidpcertname":<String_value>,

"assertionconsumerserviceurl":<String_value>,

"sendpassword":<String_value>,

"samlissuername":<String_value>,

"rejectunsignedrequests":<String_value>,

"signaturealg":<String_value>,

"digestmethod":<String_value>,

"audience":<String_value>,

"nameidformat":<String_value>,

"nameidexpr":<String_value>,

"attribute1":<String_value>,

"attribute1expr":<String_value>,

"attribute1friendlyname":<String_value>,
```

```
"attribute1format":<String_value>,

"attribute2":<String_value>,

"attribute2expr":<String_value>,

"attribute2friendlyname":<String_value>,

"attribute2format":<String_value>,

"attribute3":<String_value>,

"attribute3expr":<String_value>,

"attribute3friendlyname":<String_value>,

"attribute3format":<String_value>,

"attribute4":<String_value>,

"attribute4expr":<String_value>,

"attribute4friendlyname":<String_value>,

"attribute4format":<String_value>,

"attribute5":<String_value>,

"attribute5expr":<String_value>,

"attribute5friendlyname":<String_value>,

"attribute5format":<String_value>,

"attribute6":<String_value>,

"attribute6expr":<String_value>,

"attribute6friendlyname":<String_value>,

"attribute6format":<String_value>,

"attribute7":<String_value>,
```

```
"attribute7expr":<String_value>,

"attribute7friendlyname":<String_value>,

"attribute7format":<String_value>,

"attribute8":<String_value>,

"attribute8expr":<String_value>,

"attribute8friendlyname":<String_value>,

"attribute8format":<String_value>,

"attribute9":<String_value>,

"attribute9expr":<String_value>,

"attribute9friendlyname":<String_value>,

"attribute9format":<String_value>,

"attribute10":<String_value>,

"attribute10expr":<String_value>,

"attribute10friendlyname":<String_value>,

"attribute10format":<String_value>,

"attribute11":<String_value>,

"attribute11expr":<String_value>,

"attribute11friendlyname":<String_value>,

"attribute11format":<String_value>,

"attribute12":<String_value>,

"attribute12expr":<String_value>,

"attribute12friendlyname":<String_value>,
```

```
"attribute12format":<String_value>,

"attribute13":<String_value>,

"attribute13expr":<String_value>,

"attribute13friendlyname":<String_value>,

"attribute13format":<String_value>,

"attribute14":<String_value>,

"attribute14expr":<String_value>,

"attribute14friendlyname":<String_value>,

"attribute14format":<String_value>,

"attribute15":<String_value>,

"attribute15expr":<String_value>,

"attribute15friendlyname":<String_value>,

"attribute15format":<String_value>,

"attribute16":<String_value>,

"attribute16expr":<String_value>,

"attribute16friendlyname":<String_value>,

"attribute16format":<String_value>,

"encryptassertion":<String_value>,

"encryptionalgorithm":<String_value>,

"samlbinding":<String_value>,

"skewtime":<Integer_value>,

"serviceproviderid":<String_value>,
```

```
"signassertion":<String_value>,

"keytransportalg":<String_value>,

"splogouturl":<String_value>,

"logoutbinding":<String_value>,

"defaultauthenticationgroup":<String_value>,

"metadataurl":<String_value>,

"metadatarefreshinterval":<Integer_value>,

"signatureservice":<String_value>,

"samlsigningcertversion":<String_value>,

"samlspcertversion":<String_value>,

"acsurlrule":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationsamlidpprofile? **action=unset**
HTTP Method: POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationsamlidpprofile":{

<b>"name":<String_value>,

</b>"samlspcertname":true,

"samlidpcertname":true,

"assertionconsumerserviceurl":true,

"sendpassword":true,

"samlissuername":true,

"rejectunsignedrequests":true,

"signaturealg":true,

"digestmethod":true,

"audience":true,

"nameidformat":true,

"nameidexpr":true,

"attribute1":true,

"attribute1friendlyname":true,

"attribute1format":true,

"attribute2":true,

"attribute2friendlyname":true,

"attribute2format":true,

"attribute3":true,

"attribute3friendlyname":true,

"attribute3format":true,
```

```
"attribute4":true,

"attribute4friendlyname":true,

"attribute4format":true,

"attribute5":true,

"attribute5friendlyname":true,

"attribute5format":true,

"attribute6":true,

"attribute6friendlyname":true,

"attribute6format":true,

"attribute7":true,

"attribute7friendlyname":true,

"attribute7format":true,

"attribute8":true,

"attribute8friendlyname":true,

"attribute8format":true,

"attribute9":true,

"attribute9friendlyname":true,

"attribute9format":true,

"attribute10":true,

"attribute10friendlyname":true,

"attribute10format":true,

"attribute11":true,
```

```
"attribute11friendlyname":true,

"attribute11format":true,

"attribute12":true,

"attribute12friendlyname":true,

"attribute12format":true,

"attribute13":true,

"attribute13friendlyname":true,

"attribute13format":true,

"attribute14":true,

"attribute14friendlyname":true,

"attribute14format":true,

"attribute15":true,

"attribute15friendlyname":true,

"attribute15format":true,

"attribute16":true,

"attribute16friendlyname":true,

"attribute16format":true,

"encryptassertion":true,

"encryptionalgorithm":true,

"samlbinding":true,

"skewtime":true,

"serviceproviderid":true,
```

```
"signassertion":true,

"keytransportalg":true,

"splogouturl":true,

"logoutbinding":true,

"defaultauthenticationgroup":true,

"metadataurl":true,

"metadatarefreshinterval":true,

"signatureservice":true,

"samlsigningcertversion":true,

"samlspcertversion":true,

"acsurlrule":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationsamlidpprofile **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/authenticationsamlidpprofile? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/authenticationsamlidpprofile? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of authenticationsamlidpprofile resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/authenticationsamlidpprofile? **view=summary**

Use this query-parameter to get the summary output of authenticationsamlidpprofile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/authenticationsamlidpprofile? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authenticationsamlidpprofile resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationsamlidpprofile": [ {

"name":<String_value>,

"samlspcertname":<String_value>,

"samlidpcertname":<String_value>,

"assertionconsumerserviceurl":<String_value>,

"sendpassword":<String_value>,

"samlissuername":<String_value>,
```

```
"rejectunsignedrequests":<String_value>,

"signaturealg":<String_value>,

"digestmethod":<String_value>,

"audience":<String_value>,

"nameidformat":<String_value>,

"nameidexpr":<String_value>,

"attribute1":<String_value>,

"attribute2":<String_value>,

"attribute3":<String_value>,

"attribute4":<String_value>,

"attribute5":<String_value>,

"attribute6":<String_value>,

"attribute7":<String_value>,

"attribute8":<String_value>,

"attribute9":<String_value>,

"attribute10":<String_value>,

"attribute11":<String_value>,

"attribute12":<String_value>,

"attribute13":<String_value>,

"attribute14":<String_value>,

"attribute15":<String_value>,

"attribute16":<String_value>,
```

```
"attribute1friendlyname":<String_value>,

"attribute2friendlyname":<String_value>,

"attribute3friendlyname":<String_value>,

"attribute4friendlyname":<String_value>,

"attribute5friendlyname":<String_value>,

"attribute6friendlyname":<String_value>,

"attribute7friendlyname":<String_value>,

"attribute8friendlyname":<String_value>,

"attribute9friendlyname":<String_value>,

"attribute10friendlyname":<String_value>,

"attribute11friendlyname":<String_value>,

"attribute12friendlyname":<String_value>,

"attribute13friendlyname":<String_value>,

"attribute14friendlyname":<String_value>,

"attribute15friendlyname":<String_value>,

"attribute16friendlyname":<String_value>,

"attribute1format":<String_value>,

"attribute2format":<String_value>,

"attribute3format":<String_value>,

"attribute4format":<String_value>,

"attribute5format":<String_value>,

"attribute6format":<String_value>,
```

```
"attribute7format":<String_value>,

"attribute8format":<String_value>,

"attribute9format":<String_value>,

"attribute10format":<String_value>,

"attribute11format":<String_value>,

"attribute12format":<String_value>,

"attribute13format":<String_value>,

"attribute14format":<String_value>,

"attribute15format":<String_value>,

"attribute16format":<String_value>,

"attribute1expr":<String_value>,

"attribute2expr":<String_value>,

"attribute3expr":<String_value>,

"attribute4expr":<String_value>,

"attribute5expr":<String_value>,

"attribute6expr":<String_value>,

"attribute7expr":<String_value>,

"attribute8expr":<String_value>,

"attribute9expr":<String_value>,

"attribute10expr":<String_value>,

"attribute11expr":<String_value>,

"attribute12expr":<String_value>,
```

```
"attribute13expr":<String_value>,

"attribute14expr":<String_value>,

"attribute15expr":<String_value>,

"attribute16expr":<String_value>,

"encryptassertion":<String_value>,

"encryptionalgorithm":<String_value>,

"samlbinding":<String_value>,

"skewtime":<Integer_value>,

"serviceproviderid":<String_value>,

"signassertion":<String_value>,

"keytransportalg":<String_value>,

"splogouturl":<String_value>,

"logoutbinding":<String_value>,

"defaultauthenticationgroup":<String_value>,

"metadataurl":<String_value>,

"metadatarefreshinterval":<Integer_value>,

"metadataimportstatus":<String_value>,

"signatureservice":<String_value>,

"samlsigningcertversion":<String_value>,

"samlspcertversion":<String_value>,

"acsurlrule":<String_value>,

"_nextgenapiresource":<String_value>
```

```
}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationsamlidpprofile/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/ authenticationsamlidpprofile/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/authenticationsamlidpprofile/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of authenticationsamlidpprofile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationsamlidpprofile": [ {

"name":<String_value>,

"samlspcertname":<String_value>,
```

```
"samlidpcertname":<String_value>,

"assertionconsumerserviceurl":<String_value>,

"sendpassword":<String_value>,

"samlissuername":<String_value>,

"rejectunsignedrequests":<String_value>,

"signaturealg":<String_value>,

"digestmethod":<String_value>,

"audience":<String_value>,

"nameidformat":<String_value>,

"nameidexpr":<String_value>,

"attribute1":<String_value>,

"attribute2":<String_value>,

"attribute3":<String_value>,

"attribute4":<String_value>,

"attribute5":<String_value>,

"attribute6":<String_value>,

"attribute7":<String_value>,

"attribute8":<String_value>,

"attribute9":<String_value>,

"attribute10":<String_value>,

"attribute11":<String_value>,

"attribute12":<String_value>,
```

```
"attribute13":<String_value>,

"attribute14":<String_value>,

"attribute15":<String_value>,

"attribute16":<String_value>,

"attribute1friendlyname":<String_value>,

"attribute2friendlyname":<String_value>,

"attribute3friendlyname":<String_value>,

"attribute4friendlyname":<String_value>,

"attribute5friendlyname":<String_value>,

"attribute6friendlyname":<String_value>,

"attribute7friendlyname":<String_value>,

"attribute8friendlyname":<String_value>,

"attribute9friendlyname":<String_value>,

"attribute10friendlyname":<String_value>,

"attribute11friendlyname":<String_value>,

"attribute12friendlyname":<String_value>,

"attribute13friendlyname":<String_value>,

"attribute14friendlyname":<String_value>,

"attribute15friendlyname":<String_value>,

"attribute16friendlyname":<String_value>,

"attribute1format":<String_value>,

"attribute2format":<String_value>,
```

```
"attribute3format":<String_value>,

"attribute4format":<String_value>,

"attribute5format":<String_value>,

"attribute6format":<String_value>,

"attribute7format":<String_value>,

"attribute8format":<String_value>,

"attribute9format":<String_value>,

"attribute10format":<String_value>,

"attribute11format":<String_value>,

"attribute12format":<String_value>,

"attribute13format":<String_value>,

"attribute14format":<String_value>,

"attribute15format":<String_value>,

"attribute16format":<String_value>,

"attribute1expr":<String_value>,

"attribute2expr":<String_value>,

"attribute3expr":<String_value>,

"attribute4expr":<String_value>,

"attribute5expr":<String_value>,

"attribute6expr":<String_value>,

"attribute7expr":<String_value>,

"attribute8expr":<String_value>,
```

```
"attribute9expr":<String_value>,

"attribute10expr":<String_value>,

"attribute11expr":<String_value>,

"attribute12expr":<String_value>,

"attribute13expr":<String_value>,

"attribute14expr":<String_value>,

"attribute15expr":<String_value>,

"attribute16expr":<String_value>,

"encryptassertion":<String_value>,

"encryptionalgorithm":<String_value>,

"samlbinding":<String_value>,

"skewtime":<Integer_value>,

"serviceproviderid":<String_value>,

"signassertion":<String_value>,

"keytransportalg":<String_value>,

"splogouturl":<String_value>,

"logoutbinding":<String_value>,

"defaultauthenticationgroup":<String_value>,

"metadataurl":<String_value>,

"metadatarefreshinterval":<Integer_value>,

"metadataimportstatus":<String_value>,

"signatureservice":<String_value>,
```

```
"samlsigningcertversion":<String_value>,

"samlspcertversion":<String_value>,

"acsurlrule":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationsamlidpprofile? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationsamlidpprofile": [ { "__count": "#no"} ] }
```

authenticationsamlpolicy

Configuration for AAA Saml policy resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the SAML policy. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after SAML policy is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my authentication policy" or 'my authentication policy'). Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
rule	<String>	Read-write	Name of the Citrix ADC named rule, or an expression, that the policy uses to determine whether to attempt to authenticate the user with the SAML server. Minimum length = 1
reqaction	<String>	Read-write	Name of the SAML authentication action to be performed if the policy matches. Minimum length = 1
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationsamlpolicy **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationsamlpolicy":{

<b>"name":<String_value>,

</b><b>"rule":<String_value>,

</b><b>"reqaction":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationsamlpolicy/ name_value<String>
HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationsamlpolicy **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationsamlpolicy":{

<b>"name":<String_value>,

</b>"rule":<String_value>,

"reqaction":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationsamlpolicy? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationsamlpolicy":{

<b>"name":<String_value>,

</b>"rule":true,

"reqaction":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationsamlpolicy **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/authenticationsamlpolicy? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/authenticationsamlpolicy? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of authenticationsamlpolicy resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/authenticationsamlpolicy? **view=summary**

Use this query-parameter to get the summary output of authenticationsamlpolicy resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/authenticationsamlpolicy? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authenticationsamlpolicy resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationsamlpolicy": [ {

"name":<String_value>,

"rule":<String_value>,

"reqaction":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationsamlpolicy/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/authenticationsamlpolicy/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/authenticationsamlpolicy/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of authenticationsamlpolicy resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationsamlpolicy": [ {

"name":<String_value>,

"rule":<String_value>,

"reqaction":<String_value>,

"_nextgenapiresource":<String_value>
```

```
}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationsamlpolicy? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationsamlpolicy": [ { "__count": "#no"} ] }
```

authenticationsamlpolicy_authenticationvserver_binding

Binding object showing the authenticationvserver that can be bound to authenticationsamlpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the SAML policy. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
boundto	<String>	Read-write	The entity name to which policy is bound.
activepolicy	<Integer>	Read-only	.
priority	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationsamlpolicy_authenticationvserver_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ authenticationsamlpolicy_authenticationvserver_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of authenticationsamlpolicy_authenticationvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ authenticationsamlpolicy_authenticationvserver_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authenticationsamlpolicy_authenticationvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationsamlpolicy_authenticationvserver_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"activepolicy":<Integer_value>,

"priority":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationsamlpolicy_authenticationvserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ authenticationsamlpolicy_authenticationvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationsamlpolicy_authenticationvserver_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"activepolicy":<Integer_value>,

"priority":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationsamlpolicy_authenticationvserver_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"authenticationsamlpolicy_authenticationvserver_binding": [ { "__count":
"#no"} ] }
```

authenticationsamlpolicy_binding

Binding object which returns the resources bound to authenticationsamlpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the SAML policy. Minimum length = 1
authenticationsamlpolicy_vpnglobal_binding	<authenticationsamlpolicy_vpnglobal_binding[]>	Read-only	vpnglobal that can be bound to authenticationsamlpolicy.
authenticationsamlpolicy_vpnvserver_binding	<authenticationsamlpolicy_vpnvserver_binding[]>	Read-only	vpnvserver that can be bound to authenticationsamlpolicy.
authenticationsamlpolicy_authenticationvserver_binding	<authenticationsamlpolicy_authenticationvserver_binding[]>	Read-only	authenticationvserver that can be bound to authenticationsamlpolicy.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationsamlpolicy_binding/ name_value<String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationsamlpolicy_binding": [ {

"name":<String_value>,

"authenticationsamlpolicy_vpnglobal_binding":<authenticationsamlpolicy_vpn
global_binding[]_value>,
```

```
"authenticationsamlpolicy_authenticationvserver_binding":<authenticationsa
mlpolicy_authenticationvserver_binding[]_value>,

"authenticationsamlpolicy_vpnvserver_binding":<authenticationsamlpolicy_vp
nvserver_binding[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationsamlpolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/authenticationsamlpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationsamlpolicy_binding": [ {

"name":<String_value>,

"authenticationsamlpolicy_vpnglobal_binding":<authenticationsamlpolicy_vpn
global_binding[]_value>,
```

```
"authenticationsamlpolicy_authenticationvserver_binding":<authenticationsa
mlpolicy_authenticationvserver_binding[]_value>,

"authenticationsamlpolicy_vpnvserver_binding":<authenticationsamlpolicy_vp
nvserver_binding[]_value>

}]}
```

authenticationsamlpolicy_vpnglobal_binding

Binding object showing the vpnglobal that can be bound to authenticationsamlpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
boundto	<String>	Read-write	The entity name to which policy is bound.
name	<String>	Read-write	Name of the SAML policy. Minimum length = 1
priority	<Integer>	Read-only	.
activepolicy	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationsamlpolicy_vpnglobal_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ authenticationsamlpolicy_vpnglobal_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of authenticationsamlpolicy_vpnglobal_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ authenticationsamlpolicy_vpnglobal_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authenticationsamlpolicy_vpnglobal_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationsamlpolicy_vpnglobal_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"priority":<Integer_value>,

"activepolicy":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationsamlpolicy_vpnglobal_binding
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/authenticationsamlpolicy_vpnglobal_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationsamlpolicy_vpnglobal_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"priority":<Integer_value>,

"activepolicy":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationsamlpolicy_vpnglobal_binding/name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"authenticationsamlpolicy_vpnglobal_binding": [ { "__count": "#no"} ] }
```

authenticationsamlpolicy_vpnvserver_binding

Binding object showing the vpnvserver that can be bound to authenticationsamlpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
boundto	<String>	Read-write	The entity name to which policy is bound.
name	<String>	Read-write	Name of the SAML policy. Minimum length = 1
priority	<Integer>	Read-only	.
activepolicy	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationsamlpolicy_vpnvserver_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ authenticationsamlpolicy_vpnvserver_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of authenticationsamlpolicy_vpnvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ authenticationsamlpolicy_vpnvserver_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authenticationsamlpolicy_vpnvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationsamlpolicy_vpnvserver_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"priority":<Integer_value>,

"activepolicy":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationsamlpolicy_vpnvserver_binding
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/authenticationsamlpolicy_vpnvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationsamlpolicy_vpnvserver_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"priority":<Integer_value>,

"activepolicy":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationsamlpolicy_vpnvserver_binding/name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"authenticationsamlpolicy_vpnvserver_binding": [ { "__count": "#no"} ] }
```

authenticationsmartaccesspolicy

Configuration for SmartAccess policy resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the Smartaccess policy. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after Smartaccess policy is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			single quotation marks (for example, "my authentication policy" or 'my authentication policy'). Minimum length = 1
rule	<String>	Read-write	Name of the Citrix ADC named rule, or an expression. Minimum length = 1
action	<String>	Read-write	Name of the Smartaccess profile to use if the policy matches. Minimum length = 1
comment	<String>	Read-write	Any comments to preserve information about this policy.
hits	<Integer>	Read-only	Number of hits.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)

- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationsmartaccesspolicy **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationsmartaccesspolicy":{

<b>"name":<String_value>,

</b><b>"rule":<String_value>,

</b><b>"action":<String_value>,

</b>"comment":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationsmartaccesspolicy/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationsmartaccesspolicy **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationsmartaccesspolicy":{

<b>"name":<String_value>,

</b>"rule":<String_value>,

"action":<String_value>,

"comment":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationsmartaccesspolicy?**action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationsmartaccesspolicy":{

<b>"name":<String_value>,

</b>"comment":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationsmartaccesspolicy **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/authenticationsmartaccesspolicy?**attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/authenticationsmartaccesspolicy?**filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of authenticationsmartaccesspolicy resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/authenticationsmartaccesspolicy?**view=summary**

Use this query-parameter to get the summary output of authenticationsmartaccesspolicy resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/authenticationsmartaccesspolicy?**pagesize=#no;pageno=#no**

Use this query-parameter to get the authenticationsmartaccesspolicy resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationsmartaccesspolicy": [ {

"name":<String_value>,

"rule":<String_value>,

"action":<String_value>,

"hits":<Integer_value>,

"comment":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationsmartaccesspolicy/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/ authenticationsmartaccesspolicy/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/authenticationsmartaccesspolicy/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of authenticationsmartaccesspolicy resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationsmartaccesspolicy": [ {

"name":<String_value>,

"rule":<String_value>,

"action":<String_value>,

"hits":<Integer_value>,

"comment":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationsmartaccesspolicy? **count=yes**
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationsmartaccesspolicy": [ { "__count": "#no"} ] }
```

authenticationsmartaccesspolicy_authenticationvserver_binding

Binding object showing the authenticationvserver that can be bound to authenticationsmartaccesspolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the Smartaccess policy. Minimum length = 1
boundto	<String>	Read-write	The entity name to which policy is bound.
activepolicy	<Integer>	Read-only	.
priority	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationsmartaccesspolicy_authenticationvserver_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/authenticationsmartaccesspolicy_authenticationvserver_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of authenticationsmartaccesspolicy_authenticationvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/authenticationsmartaccesspolicy_authenticationvserver_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authenticationsmartaccesspolicy_authenticationvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationsmartaccesspolicy_authenticationvserver_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"activepolicy":<Integer_value>,

"priority":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationsmartaccesspolicy_authenticationvserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ authenticationsmartaccesspolicy_authenticationvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationsmartaccesspolicy_authenticationvserver_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"activepolicy":<Integer_value>,

"priority":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationsmartaccesspolicy_authenticationvserver_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"authenticationsmartaccesspolicy_authenticationvserver_binding":
[ { "__count": "#no"} ] }
```

authenticationsmartaccesspolicy_binding

Binding object which returns the resources bound to authenticationsmartaccesspolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the Smartaccess policy. Minimum length = 1
authenticationsmartaccesspolicy_authenticationvserver_binding	<authenticationsmartaccesspolicy_authenticationvserver_binding[]>	Read-only	authenticationvserver that can be bound to authenticationsmartaccesspolicy.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationsmartaccesspolicy_binding/name_value<String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationsmartaccesspolicy_binding": [ {

"name":<String_value>,

"authenticationsmartaccesspolicy_authenticationvserver_binding":<authentic
ationsmartaccesspolicy_authenticationvserver_binding[]_value>
```

```
}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationsmartaccesspolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/authenticationsmartaccesspolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationsmartaccesspolicy_binding": [ {

"name":<String_value>,

"authenticationsmartaccesspolicy_authenticationvserver_binding":<authentic
ationsmartaccesspolicy_authenticationvserver_binding[]_value>

}]}
```

authenticationsmartaccessprofile

Configuration for SmartAccess profile resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the Smartaccess profile. Minimum length = 1
tags	<String>	Read-write	The tag that is associated with Smartaccess profile. Minimum length = 1
comment	<String>	Read-write	Optional comment for the profile.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- UPDATE
- UNSET
- DELETE
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationsmartaccessprofile **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationsmartaccessprofile":{

<b>"name":<String_value>,

</b><b>"tags":<String_value>,
```

```
</b>"comment":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationsmartaccessprofile **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationsmartaccessprofile":{

<b>"name":<String_value>,

</b>"tags":<String_value>,

"comment":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationsmartaccessprofile?**action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationsmartaccessprofile":{

<b>"name":<String_value>,

</b>"comment":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationsmartaccessprofile/name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationsmartaccessprofile **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/authenticationsmartaccessprofile?**attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/authenticationsmartaccessprofile? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of authenticationsmartaccessprofile resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/authenticationsmartaccessprofile? **view=summary**

Use this query-parameter to get the summary output of authenticationsmartaccessprofile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/authenticationsmartaccessprofile? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authenticationsmartaccessprofile resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationsmartaccessprofile": [ {

"name":<String_value>,

"tags":<String_value>,

"comment":<String_value>,
```

```
"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationsmartaccessprofile/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/ authenticationsmartaccessprofile/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/authenticationsmartaccessprofile/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of authenticationsmartaccessprofile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationsmartaccessprofile": [ {

"name":<String_value>,
```

```
"tags":<String_value>,

"comment":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationsmartaccessprofile? **count=yes**
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationsmartaccessprofile": [ { "__count": "#no"} ] }
```

authenticationstorefrontauthaction

Configuration for Storefront authentication action resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the Storefront Authentication action. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after the profile is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my authentication action" or 'my authentication action'). Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
serverurl	<String>	Read-write	URL of the Storefront server. This is the FQDN of the Storefront server. example: https://storefront.com/. Authentication endpoints are learned dynamically by Gateway.
domain	<String>	Read-write	Domain of the server that is used for authentication. If users enter name without domain, this parameter is added to username in the authentication request to server.
defaultauthenticationgroup	<String>	Read-write	This is the default group that is chosen when the authentication succeeds in addition to extracted groups.
success	<Integer>	Read-only	.
failure	<Integer>	Read-only	.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD

- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationstorefrontauthaction **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationstorefrontauthaction":{

<b>"name":<String_value>,

</b><b>"serverurl":<String_value>,

</b>"domain":<String_value>,

"defaultauthenticationgroup":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationstorefrontauthaction/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationstorefrontauthaction **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationstorefrontauthaction":{

<b>"name":<String_value>,

</b>"serverurl":<String_value>,

"domain":<String_value>,

"defaultauthenticationgroup":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationstorefrontauthaction?**action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationstorefrontauthaction":{

<b>"name":<String_value>,

</b>"domain":true,

"defaultauthenticationgroup":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationstorefrontauthaction **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/authenticationstorefrontauthaction? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/authenticationstorefrontauthaction? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of authenticationstorefrontauthaction resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/authenticationstorefrontauthaction? **view=summary**

Use this query-parameter to get the summary output of authenticationstorefrontauthaction resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/authenticationstorefrontauthaction? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authenticationstorefrontauthaction resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationstorefrontauthaction": [ {

"name":<String_value>,

"serverurl":<String_value>,

"domain":<String_value>,

"defaultauthenticationgroup":<String_value>,

"success":<Integer_value>,

"failure":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationstorefrontauthaction/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/ authenticationstorefrontauthaction/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/authenticationstorefrontauthaction/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of authenticationstorefrontauthaction resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationstorefrontauthaction": [ {

"name":<String_value>,

"serverurl":<String_value>,

"domain":<String_value>,

"defaultauthenticationgroup":<String_value>,

"success":<Integer_value>,

"failure":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationstorefrontauthaction? **count=yes**
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationstorefrontauthaction": [ { "__count": "#no"} ] }
```

authenticationtacacsaction

Configuration for TACACS action resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the TACACS+ profile (action). Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Cannot

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			be changed after TACACS profile is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my authentication action" or 'y authentication action'). Minimum length = 1
serverip	<String>	Read-write	IP address assigned to the TACACS+ server. Minimum length = 1
serverport	<Integer>	Read-write	Port number on which the TACACS+ server listens for connections. Default value: 49 Minimum value = 1
authtimeout	<Integer>	Read-write	Number of seconds the Citrix ADC waits for a response from

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			the TACACS+ server. Default value: 3 Minimum value = 1
tacacssecret	<String>	Read-write	Key shared between the TACACS+ server and the Citrix ADC. Required for allowing the Citrix ADC to communicate with the TACACS+ server. Minimum length = 1
authorization	<String>	Read-write	Use streaming authorization on the TACACS+ server. Possible values = ON, OFF
accounting	<String>	Read-write	Whether the TACACS+ server is currently accepting accounting messages. Possible values = ON, OFF
auditfailedcmds	<String>	Read-write	The state of the TACACS+ server that will receive accounting messages. Possible values = ON, OFF

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
groupattrname	<String>	Read-write	TACACS+ group attribute name. Used for group extraction on the TACACS+ server.
defaultauthenticationgroup	<String>	Read-write	This is the default group that is chosen when the authentication succeeds in addition to extracted groups.
attribute1	<String>	Read-write	Name of the custom attribute to be extracted from server and stored at index '1' (where '1' changes for each attribute).
attribute2	<String>	Read-write	Name of the custom attribute to be extracted from server and stored at index '2' (where '2' changes for each attribute).
attribute3	<String>	Read-write	Name of the custom attribute to be extracted from server and stored at index '3' (where '3' changes for each attribute).
attribute4	<String>	Read-write	Name of the custom attribute to be extracted from server and stored at index

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			'4' (where '4' changes for each attribute).
attribute5	<String>	Read-write	Name of the custom attribute to be extracted from server and stored at index '5' (where '5' changes for each attribute).
attribute6	<String>	Read-write	Name of the custom attribute to be extracted from server and stored at index '6' (where '6' changes for each attribute).
attribute7	<String>	Read-write	Name of the custom attribute to be extracted from server and stored at index '7' (where '7' changes for each attribute).
attribute8	<String>	Read-write	Name of the custom attribute to be extracted from server and stored at index '8' (where '8' changes for each attribute).
attribute9	<String>	Read-write	Name of the custom attribute to be extracted from server and stored at index '9' (where '9'

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			changes for each attribute).
attribute10	<String>	Read-write	Name of the custom attribute to be extracted from server and stored at index '10' (where '10' changes for each attribute).
attribute11	<String>	Read-write	Name of the custom attribute to be extracted from server and stored at index '11' (where '11' changes for each attribute).
attribute12	<String>	Read-write	Name of the custom attribute to be extracted from server and stored at index '12' (where '12' changes for each attribute).
attribute13	<String>	Read-write	Name of the custom attribute to be extracted from server and stored at index '13' (where '13' changes for each attribute).
attribute14	<String>	Read-write	Name of the custom attribute to be extracted from server and stored at index '14' (where '14'

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			changes for each attribute).
attribute15	<String>	Read-write	Name of the custom attribute to be extracted from server and stored at index '15' (where '15' changes for each attribute).
attribute16	<String>	Read-write	Name of the custom attribute to be extracted from server and stored at index '16' (where '16' changes for each attribute).
attributes	<String>	Read-write	List of attribute names separated by ',' which needs to be fetched from tacacs server. Note that preceeding and trailing spaces will be removed. Attribute name can be 127 bytes and total length of this string should not cross 2047 bytes. These attributes have multi-value support separated by ',' and stored as

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			key-value pair in AAA session.
success	<Integer>	Read-only	.
failure	<Integer>	Read-only	.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationtacacsaction **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationtacacsaction":{

<b>"name":<String_value>,

</b>"serverip":<String_value>,

"serverport":<Integer_value>,

"authtimeout":<Integer_value>,

"tacacssecret":<String_value>,

"authorization":<String_value>,

"accounting":<String_value>,

"auditfailedcmds":<String_value>,

"groupattrname":<String_value>,
```

```
"defaultauthenticationgroup":<String_value>,

"attribute1":<String_value>,

"attribute2":<String_value>,

"attribute3":<String_value>,

"attribute4":<String_value>,

"attribute5":<String_value>,

"attribute6":<String_value>,

"attribute7":<String_value>,

"attribute8":<String_value>,

"attribute9":<String_value>,

"attribute10":<String_value>,

"attribute11":<String_value>,

"attribute12":<String_value>,

"attribute13":<String_value>,

"attribute14":<String_value>,

"attribute15":<String_value>,

"attribute16":<String_value>,

"attributes":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationtacacsaction/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationtacacsaction **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationtacacsaction":{

<b>"name":<String_value>,

</b>"serverip":<String_value>,

"serverport":<Integer_value>,

"authtimeout":<Integer_value>,

"tacacssecret":<String_value>,

"authorization":<String_value>,

"accounting":<String_value>,

"auditfailedcmds":<String_value>,
```

```
"groupattrname":<String_value>,

"defaultauthenticationgroup":<String_value>,

"attribute1":<String_value>,

"attribute2":<String_value>,

"attribute3":<String_value>,

"attribute4":<String_value>,

"attribute5":<String_value>,

"attribute6":<String_value>,

"attribute7":<String_value>,

"attribute8":<String_value>,

"attribute9":<String_value>,

"attribute10":<String_value>,

"attribute11":<String_value>,

"attribute12":<String_value>,

"attribute13":<String_value>,

"attribute14":<String_value>,

"attribute15":<String_value>,

"attribute16":<String_value>,

"attributes":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationtacacsaction? **action=unset**
HTTP Method: POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationtacacsaction":{

<b>"name":<String_value>,

</b>"serverip":true,

"serverport":true,

"authtimeout":true,

"tacacssecret":true,

"authorization":true,

"accounting":true,

"auditfailedcmds":true,

"groupattrname":true,

"defaultauthenticationgroup":true,

"attribute1":true,

"attribute2":true,

"attribute3":true,
```

```
"attribute4":true,

"attribute5":true,

"attribute6":true,

"attribute7":true,

"attribute8":true,

"attribute9":true,

"attribute10":true,

"attribute11":true,

"attribute12":true,

"attribute13":true,

"attribute14":true,

"attribute15":true,

"attribute16":true,

"attributes":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationtacacsaction **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/authenticationtacacsaction? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/authenticationtacacsaction? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of authenticationtacacsaction resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/authenticationtacacsaction? **view=summary**

Use this query-parameter to get the summary output of authenticationtacacsaction resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/authenticationtacacsaction? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authenticationtacacsaction resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationtacacsaction": [ {

"name":<String_value>,

"serverip":<String_value>,

"serverport":<Integer_value>,
```

```
"authtimeout":<Integer_value>,

"tacacssecret":<String_value>,

"authorization":<String_value>,

"accounting":<String_value>,

"auditfailedcmds":<String_value>,

"groupattrname":<String_value>,

"success":<Integer_value>,

"failure":<Integer_value>,

"defaultauthenticationgroup":<String_value>,

"attribute1":<String_value>,

"attribute2":<String_value>,

"attribute3":<String_value>,

"attribute4":<String_value>,

"attribute5":<String_value>,

"attribute6":<String_value>,

"attribute7":<String_value>,

"attribute8":<String_value>,

"attribute9":<String_value>,

"attribute10":<String_value>,

"attribute11":<String_value>,

"attribute12":<String_value>,

"attribute13":<String_value>,
```

```
"attribute14":<String_value>,

"attribute15":<String_value>,

"attribute16":<String_value>,

"attributes":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationtacacsaction/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/ authenticationtacacsaction/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/authenticationtacacsaction/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of authenticationtacacsaction resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationtacacsaction": [ {

"name":<String_value>,

"serverip":<String_value>,

"serverport":<Integer_value>,

"authtimeout":<Integer_value>,

"tacacssecret":<String_value>,

"authorization":<String_value>,

"accounting":<String_value>,

"auditfailedcmds":<String_value>,

"groupattrname":<String_value>,

"success":<Integer_value>,

"failure":<Integer_value>,

"defaultauthenticationgroup":<String_value>,

"attribute1":<String_value>,

"attribute2":<String_value>,

"attribute3":<String_value>,

"attribute4":<String_value>,

"attribute5":<String_value>,

"attribute6":<String_value>,

"attribute7":<String_value>,
```

```
"attribute8":<String_value>,

"attribute9":<String_value>,

"attribute10":<String_value>,

"attribute11":<String_value>,

"attribute12":<String_value>,

"attribute13":<String_value>,

"attribute14":<String_value>,

"attribute15":<String_value>,

"attribute16":<String_value>,

"attributes":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationtacacsaction? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationtacacsaction": [ { "__count": "#no"} ] }
```

authenticationtacacspolicy

Configuration for TACACS policy resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the TACACS+ policy. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after TACACS+ policy is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			name in double or single quotation marks (for example, "my authentication policy" or 'my authentication policy'). Minimum length = 1
rule	<String>	Read-write	Name of the Citrix ADC named rule, or an expression, that the policy uses to determine whether to attempt to authenticate the user with the TACACS+ server. Minimum length = 1
reqaction	<String>	Read-write	Name of the TACACS+ action to perform if the policy matches. Minimum length = 1
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET

- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.
- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationtacacspolicy **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationtacacspolicy":{

<b>"name":<String_value>,

</b><b>"rule":<String_value>,

</b>"reqaction":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationtacacspolicy/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationtacacspolicy **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationtacacspolicy":{

<b>"name":<String_value>,
```

```
</b>"rule":<String_value>,

"reqaction":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationtacacspolicy? **action=unset**
HTTP Method: POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationtacacspolicy":{

<b>"name":<String_value>,

</b>"rule":true,

"reqaction":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationtacacspolicy **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/authenticationtacacspolicy? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/authenticationtacacspolicy? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of authenticationtacacspolicy resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/authenticationtacacspolicy? **view=summary**

Use this query-parameter to get the summary output of authenticationtacacspolicy resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/authenticationtacacspolicy? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authenticationtacacspolicy resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationtacacspolicy": [ {

"name":<String_value>,

"rule":<String_value>,

"reqaction":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationtacacspolicy/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/ authenticationtacacspolicy/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/authenticationtacacspolicy/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of authenticationtacacspolicy resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationtacacspolicy": [ {

"name":<String_value>,

"rule":<String_value>,

"reqaction":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationtacacspolicy? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationtacacspolicy": [ { "__count": "#no"} ] }
```

authenticationtacacspolicy_authenticationvserver_binding

Binding object showing the authenticationvserver that can be bound to authenticationtacacspolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the TACACS+ policy. Minimum length = 1
boundto	<String>	Read-write	The entity name to which policy is bound.
activepolicy	<Integer>	Read-only	.
priority	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationtacacspolicy_authenticationvserver_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ authenticationtacacspolicy_authenticationvserver_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of authenticationtacacspolicy_authenticationvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ authenticationtacacspolicy_authenticationvserver_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authenticationtacacspolicy_authenticationvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationtacacspolicy_authenticationvserver_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"activepolicy":<Integer_value>,

"priority":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationtacacspolicy_authenticationvserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ authenticationtacacspolicy_authenticationvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationtacacspolicy_authenticationvserver_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"activepolicy":<Integer_value>,

"priority":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationtacacspolicy_authenticationvserver_binding/ name_value<String> ? **count=yes**
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"authenticationtacacspolicy_authenticationvserver_binding":
[ { "__count": "#no"} ] }
```

authenticationtacacspolicy_binding

Binding object which returns the resources bound to authenticationtacacspolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the TACACS+ policy. Minimum length = 1
authenticationtacacspolicy_authenticationvserver_binding	<authenticationtacacspolicy_authenticationvserver_binding[]>	Read-only	authenticationvserver that can be bound to authenticationtacacspolicy.
authenticationtacacspolicy_vpnglobal_binding	<authenticationtacacspolicy_vpnglobal_binding[]>	Read-only	vpnglobal that can be bound to authenticationtacacspolicy.
authenticationtacacspolicy_vpnvserver_binding	<authenticationtacacspolicy_vpnvserver_binding[]>	Read-only	vpnvserver that can be bound to authenticationtacacspolicy.
authenticationtacacspolicy_systemglobal_binding	<authenticationtacacspolicy_systemglobal_binding[]>	Read-only	systemglobal that can be bound to authenticationtacacspolicy.

Operations

(click to see Properties)

- GET

- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationtacacspolicy_binding/name_value<String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationtacacspolicy_binding": [ {

"name":<String_value>,

"authenticationtacacspolicy_vpnvserver_binding":<authenticationtacacspolic
y_vpnvserver_binding[]_value>,

"authenticationtacacspolicy_authenticationvserver_binding":<authentication
tacacspolicy_authenticationvserver_binding[]_value>,

"authenticationtacacspolicy_systemglobal_binding":<authenticationtacacspol
icy_systemglobal_binding[]_value>,

"authenticationtacacspolicy_vpnglobal_binding":<authenticationtacacspolicy
_vpnglobal_binding[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationtacacspolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/authenticationtacacspolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationtacacspolicy_binding": [ {

"name":<String_value>,

"authenticationtacacspolicy_vpnvserver_binding":<authenticationtacacspolic
y_vpnvserver_binding[]_value>,

"authenticationtacacspolicy_authenticationvserver_binding":<authentication
tacacspolicy_authenticationvserver_binding[]_value>,

"authenticationtacacspolicy_systemglobal_binding":<authenticationtacacspol
icy_systemglobal_binding[]_value>,

"authenticationtacacspolicy_vpnglobal_binding":<authenticationtacacspolicy
_vpnglobal_binding[]_value>

}]}
```

authenticationtacacspolicy_systemglobal_binding

Binding object showing the systemglobal that can be bound to authenticationtacacspolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
boundto	<String>	Read-write	The entity name to which policy is bound.
name	<String>	Read-write	Name of the TACACS+ policy.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum length = 1
priority	<Integer>	Read-only	.
activepolicy	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationtacacspolicy_systemglobal_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/authenticationtacacspolicy_systemglobal_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of authenticationtacacspolicy_systemglobal_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ authenticationtacacspolicy_systemglobal_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authenticationtacacspolicy_systemglobal_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationtacacspolicy_systemglobal_binding": [ {

"boundto":<String_value>,
```

```
"name":<String_value>,

"priority":<Integer_value>,

"activepolicy":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationtacacspolicy_systemglobal_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ authenticationtacacspolicy_systemglobal_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationtacacspolicy_systemglobal_binding": [ {

"boundto":<String_value>,

"name":<String_value>,
```

```
"priority":<Integer_value>,

"activepolicy":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationtacacspolicy_systemglobal_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"authenticationtacacspolicy_systemglobal_binding": [ { "__count":
"#no"} ] }
```

authenticationtacacspolicy_vpnglobal_binding

Binding object showing the vpnglobal that can be bound to authenticationtacacspolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the TACACS+ policy. Minimum length = 1
boundto	<String>	Read-write	The entity name to which policy is bound.
priority	<Integer>	Read-only	.
activepolicy	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationtacacspolicy_vpnglobal_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ authenticationtacacspolicy_vpnglobal_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of authenticationtacacspolicy_vpnglobal_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ authenticationtacacspolicy_vpnglobal_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authenticationtacacspolicy_vpnglobal_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationtacacspolicy_vpnglobal_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"priority":<Integer_value>,

"activepolicy":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationtacacspolicy_vpnglobal_binding
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/authenticationtacacspolicy_vpnglobal_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationtacacspolicy_vpnglobal_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"priority":<Integer_value>,

"activepolicy":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationtacacspolicy_vpnglobal_binding/name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"authenticationtacacspolicy_vpnglobal_binding": [ { "__count": "#no"} ] }
```

authenticationtacacspolicy_vpnvserver_binding

Binding object showing the vpnvserver that can be bound to authenticationtacacspolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the TACACS+ policy. Minimum length = 1
boundto	<String>	Read-write	The entity name to which policy is bound.
activepolicy	<Integer>	Read-only	.
priority	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationtacacspolicy_vpnvserver_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/authenticationtacacspolicy_vpnvserver_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of authenticationtacacspolicy_vpnvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ authenticationtacacspolicy_vpnvserver_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authenticationtacacspolicy_vpnvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationtacacspolicy_vpnvserver_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"activepolicy":<Integer_value>,

"priority":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationtacacspolicy_vpnvserver_binding
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/authenticationtacacspolicy_vpnvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationtacacspolicy_vpnvserver_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"activepolicy":<Integer_value>,

"priority":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationtacacspolicy_vpnvserver_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"authenticationtacacspolicy_vpnvserver_binding": [ { "__count":
"#no"} ] }
```

authenticationvserver

Configuration for authentication virtual server resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the new authentication virtual server. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Can be changed after the authentication virtual server is added by using the rename authentication vserver command. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			"my authentication policy" or 'my authentication policy'). Minimum length = 1
servicetype	<String>	Read-write	Protocol type of the authentication virtual server. Always SSL. Default value: SSL Possible values = SSL
ipv46	<String>	Read-write	IP address of the authentication virtual server, if a single IP address is assigned to the virtual server. Minimum length = 1
range	<Integer>	Read-write	If you are creating a series of virtual servers with a range of IP addresses assigned to them, the length of the range. The new range of authentication virtual servers will have IP addresses consecutively numbered, starting with the primary address specified

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			with the IP Address parameter. Default value: 1 Minimum value = 1
port	<Integer>	Read-write	TCP port on which the virtual server accepts connections. Range 1 - 65535 * in CLI is represented as 65535 in NITRO API
state	<String>	Read-write	Initial state of the new virtual server. Default value: ENABLED Possible values = ENABLED, DISABLED
authentication	<String>	Read-write	Require users to be authenticated before sending traffic through this virtual server. Default value: ON Possible values = ON, OFF
authenticationdomain	<String>	Read-write	The domain of the authentication cookie set by Authentication vserver.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum length = 3 Maximum length = 252
comment	<String>	Read-write	Any comments associated with this virtual server.
td	<Integer>	Read-write	Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0. Minimum value = 0 Maximum value = 4094
appflowlog	<String>	Read-write	Log AppFlow flow information. Default value: ENABLED Possible values = ENABLED, DISABLED
maxloginattempts	<Integer>	Read-write	Maximum Number of login Attempts. Minimum value = 1 Maximum value = 255

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
failedlogintimeout	<Integer>	Read-write	Number of minutes an account will be locked if user exceeds maximum permissible attempts. Minimum value = 1
certkeynames	<String>	Read-write	Name of the certificate key that was bound to the corresponding SSL virtual server as the Certificate Authority for the device certificate. Minimum length = 1 Maximum length = 127
samesite	<String>	Read-write	SameSite attribute value for Cookies generated in AAATM context. This attribute value will be appended only for the cookies which are specified in the builtin patset ns_cookies_samesite. Possible values = None, LAX, STRICT
wasmmodule	<String>	Read-write	Name of the WASM module to assign to this virtual server.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
newname	<String>	Read-write	New name of the authentication virtual server. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, 'my authentication policy' or "my authentication policy"). Minimum length = 1
ip	<String>	Read-only	The Virtual IP address of the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			authentication vserver.
value	<String>	Read-only	Indicates whether or not the certificate is bound or if SSL offload is disabled. Possible values = Certkey/ Certkeybundle/Vault not bound/Cert-store not usable, SSL feature disabled
type	<String>	Read-only	The type of Virtual Server, e.g. CONTENT based or ADDRESS based. Possible values = CONTENT, ADDRESS
curstate	<String>	Read-only	The current state of the Virtual server, e.g. UP, DOWN, BUSY, etc. Possible values = UP, DOWN, UNKNOWN, BUSY, OUT OF SERVICE, GOING OUT OF SERVICE, DOWN WHEN GOING OUT OF SERVICE, NS_EMPTY_STR, Unknown, DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
status	<Integer>	Read-only	Whether or not this vserver responds to ARPs and whether or not round-robin selection is temporarily in effect.
cachetype	<String>	Read-only	Virtual server's cache type. The options are: TRANSPARENT, REVERSE and FORWARD. Possible values = TRANSPARENT, REVERSE, FORWARD
redirect	<String>	Read-only	The cache redirect policy. The valid redirect policies are: l. CACHE - Directs all requests to the cache. 2. POLICY - Applies cache redirection policy to determine whether the request should be directed to the cache or origin. This is the default setting.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			3. ORIGIN - Directs all requests to the origin server. Possible values = CACHE, POLICY, ORIGIN
precedence	<String>	Read-only	This argument is used only when configuring content switching on the specified virtual server. This is applicable only if both the URL and RULE-based policies have been configured on the same virtual server. It specifies the type of policy (URL or RULE) that takes precedence on the content switching virtual server. The default setting is RULE. l URL - In this case, the incoming request is matched against the URL-based policies before the rule-based policies.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			l RULE - In this case, the incoming request is matched against the rule-based policies before the URL-based policies. For all URL-based policies, the precedence hierarchy is: 1. Domain and exact URL 2. Domain, prefix and suffix 3. Domain and suffix 4. Domain and prefix 5. Domain only 6. Exact URL 7. Prefix and suffix 8. Suffix only 9. Prefix only 10. Default. Possible values = RULE, URL

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
redirecturl	<String>	Read-only	The URL where traffic is redirected if the virtual server in system becomes unavailable. WARNING! Make sure that the domain you specify in the URL does not match the domain specified in the -d domainName argument of the ###add cs policy### command. If the same domain is specified in both arguments, the request will be continuously redirected to the same unavailable virtual server in the system. If so, the user may not get the requested content.
curaaausers	<Integer>	Read-only	The number of current users logged in to this vserver.
policy	<String>	Read-only	The name of the policy, if any, bound to the authentication vserver.
servicename	<String>	Read-only	The name of the service, if any, to which the vserver policy is bound.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
weight	<Integer>	Read-only	Weight for this service, if any. This weight is used when the system performs load balancing, giving greater priority to a specific service. It is useful when the services bound to a virtual server are of different capacity.
cachevserver	<String>	Read-only	The name of the default target cache virtual server, if any, to which requests are redirected.
backupvserver	<String>	Read-only	The name of the backup vpn virtual server for this vpn virtual server.
clttimeout	<Integer>	Read-only	The idle time, if any, in seconds after which the client connection is terminated.
somethod	<String>	Read-only	VPN client applications are allocated from a block of Intranet IP addresses. That block may be exhausted after a certain number of connections. This switch specifies the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			method used to determine whether or not a new connection will spillover, or exhaust, the allocated block of Intranet IP addresses for that application. Possible values are CONNECTION or DYNAMICCONNECTION. CONNECTION means that a static integer value is the hard limit for the spillover threshold. The spillover threshold is described below. DYNAMICCONNECTION means that the spillover threshold is set according to the maximum number of connections defined for the vpn vserver.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = CONNECTION, DYNAMICCONNECTION, BANDWIDTH, HEALTH, LLMQUOTA, NONE
sothreshold	<Integer>	Read-only	VPN client applications are allocated from a block of Intranet IP addresses. That block may be exhausted after a certain number of connections. The value of this option is number of client connections after which the Mapped IP address is used as the client source IP address instead of an address from the allocated block of Intranet IP addresses.
sopersistence	<String>	Read-only	Whether or not cookie-based site persistance is enabled for this VPN vserver. Possible values are 'ConnectionProxy',

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			HTTPRedirect, or NONE. Possible values = ENABLED, DISABLED
sopersistencetimeout	<Integer>	Read-only	The timeout, if any, for cookie-based site persistance of this VPN vserver.
priority	<Integer>	Read-only	The priority, if any, of the vpn vserver policy.
downstateflush	<String>	Read-only	Perform delayed clean up of connections on this vserver. Possible values = ENABLED, DISABLED
bindpoint	<String>	Read-only	Bindpoint to which the policy is bound. Possible values = REQUEST, RESPONSE, ICA_REQUEST, OTHERTCP_REQUEST, AAA_REQUEST, AAA_RESPONSE
disableprimaryondown	<String>	Read-only	Tells whether traffic will continue reaching backup vservers even after

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			primary comes UP from DOWN state. Possible values = ENABLED, DISABLED
listenpolicy	<String>	Read-only	Listenpolicy configured for authentication vserver.
listenpriority	<Integer>	Read-only	Priority of listen policy for authentication vserver.
tcpprofilename	<String>	Read-only	The name of the TCP profile.
httpprofilename	<String>	Read-only	Name of the HTTP profile.
vstype	<Integer>	Read-only	Virtual Server Type, e.g. Load Balancing, Content Switch, Cache Redirection.
ngname	<String>	Read-only	Nodegroup devno to which this authentication vsever belongs to.
secondary	<Boolean>	Read-only	Bind the authentication policy to the secondary chain. Provides for multifactor authentication in which a user must authenticate via

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			both a primary authentication method and, afterward, via a secondary authentication method. Because user groups are aggregated across authentication systems, usernames must be the same on all authentication servers. Passwords can be different.
groupextraction	<Boolean>	Read-only	Bind the Authentication policy to a tertiary chain which will be used only for group extraction. The user will not authenticate against this server, and this will only be called if primary and/or secondary authentication has succeeded.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- ENABLE
- DISABLE
- GET (ALL)
- GET
- COUNT
- RENAME

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationvserver **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationvserver":{

<b>"name":<String_value>,

</b><b>"servicetype":<String_value>,

</b>"ipv46":<String_value>,

"range":<Integer_value>,

"port":<Integer_value>,

"state":<String_value>,

"authentication":<String_value>,

"authenticationdomain":<String_value>,

"comment":<String_value>,

"td":<Integer_value>,

"appflowlog":<String_value>,

"maxloginattempts":<Integer_value>,

"failedlogintimeout":<Integer_value>,

"certkeynames":<String_value>,

"samesite":<String_value>,
```

```
"wasmmodule":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationvserver/ name_value<String>
HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationvserver **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationvserver":{

<b>"name":<String_value>,

</b>"ipv46":<String_value>,

"authentication":<String_value>,

"authenticationdomain":<String_value>,
```

```
"comment":<String_value>,

"appflowlog":<String_value>,

"maxloginattempts":<Integer_value>,

"failedlogintimeout":<Integer_value>,

"certkeynames":<String_value>,

"samesite":<String_value>,

"wasmmodule":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationvserver? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationvserver":{

<b>"name":<String_value>,

</b>"authenticationdomain":true,

"maxloginattempts":true,
```

```
"wasmmodule":true,

"authentication":true,

"comment":true,

"appflowlog":true,

"failedlogintimeout":true,

"certkeynames":true,

"samesite":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

ENABLE

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationvserver? **action=enable HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationvserver":{

<b>"name":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DISABLE

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationvserver? **action=disable HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationvserver":{

<b>"name":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

RENAME

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationvserver? **action=rename HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationvserver":{

<b>"name":<String_value>,
```

```
</b><b>"newname":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationvserver **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/authenticationvserver? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/authenticationvserver? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of authenticationvserver resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/authenticationvserver? **view=summary**

Use this query-parameter to get the summary output of authenticationvserver resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/authenticationvserver? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authenticationvserver resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationvserver": [ {

"name":<String_value>,

"ip":<String_value>,

"td":<Integer_value>,

"ipv46":<String_value>,

"value":<String_value>,

"port":<Integer_value>,

"range":<Integer_value>,

"servicetype":<String_value>,

"type":<String_value>,

"curstate":<String_value>,

"status":<Integer_value>,

"cachetype":<String_value>,

"redirect":<String_value>,

"precedence":<String_value>,

"redirecturl":<String_value>,

"authentication":<String_value>,
```

```
"curaaausers":<Integer_value>,

"authenticationdomain":<String_value>,

"policyname":<String_value>,

"policy":<String_value>,

"servicename":<String_value>,

"weight":<Integer_value>,

"cachevserver":<String_value>,

"backupvserver":<String_value>,

"clttimeout":<Integer_value>,

"somethod":<String_value>,

"sothreshold":<Integer_value>,

"sopersistence":<String_value>,

"sopersistencetimeout":<Integer_value>,

"priority":<Integer_value>,

"downstateflush":<String_value>,

"bindpoint":<String_value>,

"disableprimaryondown":<String_value>,

"listenpolicy":<String_value>,

"listenpriority":<Integer_value>,

"tcpprofilename":<String_value>,

"httpprofilename":<String_value>,

"comment":<String_value>,
```

```
"appflowlog":<String_value>,

"vstype":<Integer_value>,

"ngname":<String_value>,

"maxloginattempts":<Integer_value>,

"failedlogintimeout":<Integer_value>,

"secondary":<Boolean_value>,

"groupextraction":<Boolean_value>,

"certkeynames":<String_value>,

"samesite":<String_value>,

"wasmmodule":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationvserver/ name_value<String>
Query-parameters: attrs http:// <netscaler-ip-address> /nitro/v1/config/authenticationvserver/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/authenticationvserver/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of authenticationvserver resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationvserver": [ {

"name":<String_value>,

"ip":<String_value>,

"td":<Integer_value>,

"ipv46":<String_value>,

"value":<String_value>,

"port":<Integer_value>,

"range":<Integer_value>,

"servicetype":<String_value>,

"type":<String_value>,

"curstate":<String_value>,

"status":<Integer_value>,

"cachetype":<String_value>,

"redirect":<String_value>,
```

```
"precedence":<String_value>,

"redirecturl":<String_value>,

"authentication":<String_value>,

"curaaausers":<Integer_value>,

"authenticationdomain":<String_value>,

"policyname":<String_value>,

"policy":<String_value>,

"servicename":<String_value>,

"weight":<Integer_value>,

"cachevserver":<String_value>,

"backupvserver":<String_value>,

"clttimeout":<Integer_value>,

"somethod":<String_value>,

"sothreshold":<Integer_value>,

"sopersistence":<String_value>,

"sopersistencetimeout":<Integer_value>,

"priority":<Integer_value>,

"downstateflush":<String_value>,

"bindpoint":<String_value>,

"disableprimaryondown":<String_value>,

"listenpolicy":<String_value>,

"listenpriority":<Integer_value>,
```

```
"tcpprofilename":<String_value>,

"httpprofilename":<String_value>,

"comment":<String_value>,

"appflowlog":<String_value>,

"vstype":<Integer_value>,

"ngname":<String_value>,

"maxloginattempts":<Integer_value>,

"failedlogintimeout":<Integer_value>,

"secondary":<Boolean_value>,

"groupextraction":<Boolean_value>,

"certkeynames":<String_value>,

"samesite":<String_value>,

"wasmmodule":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationvserver? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationvserver": [ { "__count": "#no"} ] }
```

authenticationvserver_auditnslogpolicy_binding

Binding object showing the auditnslogpolicy that can be bound to authenticationvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
priority	<Integer>	Read-write	The priority, if any, of the vpn vserver policy.
bindpoint	<String>	Read-write	Bind point to which to bind the policy. Applies only to rewrite and cache policies. If you do not set this parameter, the policy is bound to REQ_DEFAULT or RES_DEFAULT, depending on whether the policy rule is a response-time or a request-time expression. Possible values = REQUEST, RESPONSE,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			ICA_REQUEST, OTHERTCP_REQUEST, AAA_REQUEST, AAA_RESPONSE
name	<String>	Read-write	Name of the authentication virtual server to which to bind the policy. Minimum length = 1
secondary	<Boolean>	Read-write	Applicable only while bindind classic authentication policy as advance authentication policy use nFactor.
nextfactor	<String>	Read-write	Applicable only while binding advance authentication policy as classic authentication policy does not support nFactor.
groupextraction	<Boolean>	Read-write	Applicable only while bindind classic authentication policy as advance authentication policy use nFactor.
gotopriorityexpression	<String>	Read-write	Applicable only to advance authentication policy. Expression or other value specifying the next policy to be evaluated if the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			current policy evaluates to TRUE. Specify one of the following values: * NEXT - Evaluate the policy with the next higher priority number. * END - End policy evaluation. * USE_INVOCATION_RESULT - Applicable if this policy invokes another policy label. If the final goto in the invoked policy label has a value of END, the evaluation stops. If the final goto is anything other than END, the current policy label performs a NEXT. * An expression that evaluates to a number. If you specify an expression, the number to which it evaluates determines the next policy to evaluate, as follows: * If the expression evaluates to a higher numbered priority, the policy with that priority is evaluated next. * If the expression evaluates to the priority of the current policy, the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			policy with the next higher numbered priority is evaluated next. * If the expression evaluates to a priority number that is numerically higher than the highest numbered priority, policy evaluation ends. An UNDEF event is triggered if: * The expression is invalid. * The expression evaluates to a priority number that is numerically lower than the current policy's priority. * The expression evaluates to a priority number that is between the current policy's priority number (say, 30) and the highest priority number (say, 100), but does not match any configured priority number (for example, the expression evaluates to the number 85). This example assumes that the priority number increments by 10 for every successive policy, and therefore a priority number of

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			85 does not exist in the policy label.
policy	<String>	Read-write	The name of the policy, if any, bound to the authentication vserver.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/authenticationvserver_auditnslogpolicy_binding
HTTP Method: PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"authenticationvserver_auditnslogpolicy_binding":{

<b>"name":<String_value>,

</b>"policy":<String_value>,

"priority":<Integer_value>,

"secondary":<Boolean_value>,

"groupextraction":<Boolean_value>,

"nextfactor":<String_value>,

"gotopriorityexpression":<String_value>,

"bindpoint":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_auditnslogpolicy_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/authenticationvserver_auditnslogpolicy_binding/ name_value<String> ? **args=policy: <String_value> ,secondary: <Boolean_value> ,groupextraction: <Boolean_value> ,bindpoint: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_auditnslogpolicy_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/authenticationvserver_auditnslogpolicy_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of authenticationvserver_auditnslogpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_auditnslogpolicy_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authenticationvserver_auditnslogpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationvserver_auditnslogpolicy_binding": [ {

"priority":<Integer_value>,

"bindpoint":<String_value>,

"name":<String_value>,

"secondary":<Boolean_value>,

"nextfactor":<String_value>,

"groupextraction":<Boolean_value>,

"gotopriorityexpression":<String_value>,

"policy":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationvserver_auditnslogpolicy_binding
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_auditnslogpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationvserver_auditnslogpolicy_binding": [ {

"priority":<Integer_value>,

"bindpoint":<String_value>,

"name":<String_value>,

"secondary":<Boolean_value>,

"nextfactor":<String_value>,

"groupextraction":<Boolean_value>,

"gotopriorityexpression":<String_value>,

"policy":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_auditnslogpolicy_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"authenticationvserver_auditnslogpolicy_binding": [ { "__count":
"#no"} ] }
```

authenticationvserver_auditsyslogpolicy_binding

Binding object showing the auditsyslogpolicy that can be bound to authenticationvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
gotopriorityexpression	<String>	Read-write	Applicable only to advance authentication policy. Expression or other value specifying the next policy to be evaluated if the current policy evaluates to TRUE. Specify one of the following values: * NEXT - Evaluate the policy with the next

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			higher priority number. * END - End policy evaluation. * USE_INVOCATION_RESULT - Applicable if this policy invokes another policy label. If the final goto in the invoked policy label has a value of END, the evaluation stops. If the final goto is anything other than END, the current policy label performs a NEXT. * An expression that evaluates to a number. If you specify an expression, the number to which it evaluates determines the next policy to evaluate, as follows: * If the expression evaluates to a higher numbered priority, the policy with that priority is evaluated next. * If the expression evaluates to the priority of the current policy, the policy with the next higher numbered priority is evaluated next. * If the expression evaluates to a priority number

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			that is numerically higher than the highest numbered priority, policy evaluation ends. An UNDEF event is triggered if: * The expression is invalid. * The expression evaluates to a priority number that is numerically lower than the current policy's priority. * The expression evaluates to a priority number that is between the current policy's priority number (say, 30) and the highest priority number (say, 100), but does not match any configured priority number (for example, the expression evaluates to the number 85). This example assumes that the priority number increments by 10 for every successive policy, and therefore a priority number of 85 does not exist in the policy label.
policy	<String>	Read-write	The name of the policy, if any, bound

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			to the authentication vserver.
nextfactor	<String>	Read-write	Applicable only while binding advance authentication policy as classic authentication policy does not support nFactor.
groupextraction	<Boolean>	Read-write	Applicable only while bindind classic authentication policy as advance authentication policy use nFactor.
priority	<Integer>	Read-write	The priority, if any, of the vpn vserver policy.
bindpoint	<String>	Read-write	Bind point to which to bind the policy. Applies only to rewrite and cache policies. If you do not set this parameter, the policy is bound to REQ_DEFAULT or RES_DEFAULT, depending on whether the policy rule is a response-time or a request-time expression. Possible values = REQUEST, RESPONSE, ICA_REQUEST, OTHERTCP_REQU

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			EST, AAA_REQUEST, AAA_RESPONSE
name	<String>	Read-write	Name of the authentication virtual server to which to bind the policy. Minimum length = 1
secondary	<Boolean>	Read-write	Applicable only while bindind classic authentication policy as advance authentication policy use nFactor.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/authenticationvserver_auditsyslogpolicy_binding
HTTP Method: PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"authenticationvserver_auditsyslogpolicy_binding":{

<b>"name":<String_value>,

</b>"policy":<String_value>,

"priority":<Integer_value>,

"secondary":<Boolean_value>,

"groupextraction":<Boolean_value>,
```

```
"nextfactor":<String_value>,

"gotopriorityexpression":<String_value>,

"bindpoint":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_auditsyslogpolicy_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/authenticationvserver_auditsyslogpolicy_binding/ name_value<String> ? **args=policy: <String_value> ,secondary: <Boolean_value> ,groupextraction: <Boolean_value> ,bindpoint: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_auditsyslogpolicy_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/authenticationvserver_auditsyslogpolicy_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of authenticationvserver_auditsyslogpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_auditsyslogpolicy_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authenticationvserver_auditsyslogpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationvserver_auditsyslogpolicy_binding": [ {

"gotopriorityexpression":<String_value>,

"policy":<String_value>,

"nextfactor":<String_value>,

"groupextraction":<Boolean_value>,

"priority":<Integer_value>,

"bindpoint":<String_value>,

"name":<String_value>,

"secondary":<Boolean_value>
```

```
}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_auditsyslogpolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_auditsyslogpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationvserver_auditsyslogpolicy_binding": [ {

"gotopriorityexpression":<String_value>,

"policy":<String_value>,

"nextfactor":<String_value>,

"groupextraction":<Boolean_value>,

"priority":<Integer_value>,
```

```
"bindpoint":<String_value>,

"name":<String_value>,

"secondary":<Boolean_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_auditsyslogpolicy_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"authenticationvserver_auditsyslogpolicy_binding": [ { "__count":
"#no"} ] }
```

authenticationvserver_authenticationcertpolicy_binding

Binding object showing the authenticationcertpolicy that can be bound to authenticationvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
groupextraction	<Boolean>	Read-write	Applicable only while bindind classic authentication policy as advance authentication policy use nFactor.
nextfactor	<String>	Read-write	Applicable only while binding advance authentication policy as classic authentication policy does not support nFactor.
policy	<String>	Read-write	The name of the policy, if any, bound to the authentication vserver.
gotopriorityexpression	<String>	Read-write	Applicable only to advance authentication policy. Expression or other value specifying the next policy to be evaluated if the current policy evaluates to TRUE. Specify one of the following values: * NEXT - Evaluate the policy with the next higher priority number. * END - End policy evaluation. * USE_INVOCATION_RESULT - Applicable if this policy invokes another policy label. If the final goto in the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			invoked policy label has a value of END, the evaluation stops. If the final goto is anything other than END, the current policy label performs a NEXT. * An expression that evaluates to a number. If you specify an expression, the number to which it evaluates determines the next policy to evaluate, as follows: * If the expression evaluates to a higher numbered priority, the policy with that priority is evaluated next. * If the expression evaluates to the priority of the current policy, the policy with the next higher numbered priority is evaluated next. * If the expression evaluates to a priority number that is numerically higher than the highest numbered priority, policy evaluation ends. An UNDEF event is triggered if: * The expression is invalid.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			* The expression evaluates to a priority number that is numerically lower than the current policy's priority. * The expression evaluates to a priority number that is between the current policy's priority number (say, 30) and the highest priority number (say, 100), but does not match any configured priority number (for example, the expression evaluates to the number 85). This example assumes that the priority number increments by 10 for every successive policy, and therefore a priority number of 85 does not exist in the policy label.
secondary	<Boolean>	Read-write	Bind the authentication policy to the secondary chain. Provides for multifactor authentication in which a user must authenticate via both a primary authentication method and,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			afterward, via a secondary authentication method. Because user groups are aggregated across authentication systems, usernames must be the same on all authentication servers. Passwords can be different.
name	<String>	Read-write	Name of the authentication virtual server to which to bind the policy. Minimum length = 1
bindpoint	<String>	Read-write	Bind point to which to bind the policy. Applies only to rewrite and cache policies. If you do not set this parameter, the policy is bound to REQ_DEFAULT or RES_DEFAULT, depending on whether the policy rule is a response-time or a request-time expression. Possible values = REQUEST, RESPONSE, ICA_REQUEST, OTHERTCP_REQUEST,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			AAA_REQUEST, AAA_RESPONSE
priority	<Integer>	Read-write	The priority, if any, of the vpn vserver policy.
acttype	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/ authenticationvserver_authenticationcertpolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"authenticationvserver_authenticationcertpolicy_binding":{

<b>"name":<String_value>,

</b>"policy":<String_value>,

"priority":<Integer_value>,

"secondary":<Boolean_value>,

"groupextraction":<Boolean_value>,

"nextfactor":<String_value>,

"gotopriorityexpression":<String_value>,

"bindpoint":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_authenticationcertpolicy_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_authenticationcertpolicy_binding/ name_value<String> ? **args=policy: <String_value> ,secondary: <Boolean_value> ,groupextraction: <Boolean_value> ,bindpoint: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_authenticationcertpolicy_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_authenticationcertpolicy_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of authenticationvserver_authenticationcertpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_authenticationcertpolicy_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authenticationvserver_authenticationcertpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationvserver_authenticationcertpolicy_binding": [ {

"groupextraction":<Boolean_value>,

"nextfactor":<String_value>,

"policy":<String_value>,

"gotopriorityexpression":<String_value>,

"secondary":<Boolean_value>,

"name":<String_value>,

"bindpoint":<String_value>,

"priority":<Integer_value>,

"acttype":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_authenticationcertpolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_authenticationcertpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationvserver_authenticationcertpolicy_binding": [ {

"groupextraction":<Boolean_value>,

"nextfactor":<String_value>,

"policy":<String_value>,

"gotopriorityexpression":<String_value>,

"secondary":<Boolean_value>,

"name":<String_value>,
```

```
"bindpoint":<String_value>,

"priority":<Integer_value>,

"acttype":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_authenticationcertpolicy_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"authenticationvserver_authenticationcertpolicy_binding": [ { "__count":
"#no"} ] }
```

authenticationvserver_authenticationldappolicy_binding

Binding object showing the authenticationldappolicy that can be bound to authenticationvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the authentication virtual server to which to bind the policy. Minimum length = 1
secondary	<Boolean>	Read-write	Bind the authentication policy to the secondary chain. Provides for multifactor authentication in which a user must authenticate via both a primary authentication method and, afterward, via a secondary authentication method. Because user groups are aggregated across authentication systems, usernames must be the same on all authentication servers. Passwords can be different.
priority	<Integer>	Read-write	The priority, if any, of the vpn vserver policy.
bindpoint	<String>	Read-write	Bind point to which to bind the policy. Applies only to rewrite and cache policies. If you do not set this parameter, the policy is bound to

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			REQ_DEFAULT or RES_DEFAULT, depending on whether the policy rule is a response-time or a request-time expression. Possible values = REQUEST, RESPONSE, ICA_REQUEST, OTHERTCP_REQUEST, AAA_REQUEST, AAA_RESPONSE
gotopriorityexpression	<String>	Read-write	Applicable only to advance authentication policy. Expression or other value specifying the next policy to be evaluated if the current policy evaluates to TRUE. Specify one of the following values: * NEXT - Evaluate the policy with the next higher priority number. * END - End policy evaluation. * USE_INVOCATION_RESULT - Applicable if this policy invokes another policy label. If the final goto in the invoked policy label has a value of END, the evaluation stops.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			If the final goto is anything other than END, the current policy label performs a NEXT. * An expression that evaluates to a number. If you specify an expression, the number to which it evaluates determines the next policy to evaluate, as follows: * If the expression evaluates to a higher numbered priority, the policy with that priority is evaluated next. * If the expression evaluates to the priority of the current policy, the policy with the next higher numbered priority is evaluated next. * If the expression evaluates to a priority number that is numerically higher than the highest numbered priority, policy evaluation ends. An UNDEF event is triggered if: * The expression is invalid. * The expression evaluates to a priority number that

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			is numerically lower than the current policy's priority. * The expression evaluates to a priority number that is between the current policy's priority number (say, 30) and the highest priority number (say, 100), but does not match any configured priority number (for example, the expression evaluates to the number 85). This example assumes that the priority number increments by 10 for every successive policy, and therefore a priority number of 85 does not exist in the policy label.
policy	<String>	Read-write	The name of the policy, if any, bound to the authentication vserver.
groupextraction	<Boolean>	Read-write	Bind the Authentication policy to a tertiary chain which will be used only for group extraction. The user will not authenticate against this server, and this will only be

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			called if primary and/ or secondary authentication has succeeded.
nextfactor	<String>	Read-write	Applicable only while binding advance authentication policy as classic authentication policy does not support nFactor.
acttype	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.
- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of

creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/ authenticationvserver_authenticationldappolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"authenticationvserver_authenticationldappolicy_binding":{

<b>"name":<String_value>,

</b>"policy":<String_value>,

"priority":<Integer_value>,

"secondary":<Boolean_value>,

"groupextraction":<Boolean_value>,

"nextfactor":<String_value>,
```

```
"gotopriorityexpression":<String_value>,

"bindpoint":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_authenticationldappolicy_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_authenticationldappolicy_binding/ name_value<String> ? **args=policy: <String_value> ,secondary: <Boolean_value> ,groupextraction: <Boolean_value> ,bindpoint: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_authenticationldappolicy_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_authenticationldappolicy_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of authenticationvserver_authenticationldappolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_authenticationldappolicy_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authenticationvserver_authenticationldappolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationvserver_authenticationldappolicy_binding": [ {

"name":<String_value>,

"secondary":<Boolean_value>,

"priority":<Integer_value>,

"bindpoint":<String_value>,

"gotopriorityexpression":<String_value>,

"policy":<String_value>,

"groupextraction":<Boolean_value>,

"nextfactor":<String_value>,
```

```
"acttype":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_authenticationldappolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_authenticationldappolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationvserver_authenticationldappolicy_binding": [ {

"name":<String_value>,

"secondary":<Boolean_value>,

"priority":<Integer_value>,

"bindpoint":<String_value>,
```

```
"gotopriorityexpression":<String_value>,

"policy":<String_value>,

"groupextraction":<Boolean_value>,

"nextfactor":<String_value>,

"acttype":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_authenticationldappolicy_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"authenticationvserver_authenticationldappolicy_binding": [ { "__count":
"#no"} ] }
```

authenticationvserver_authenticationlocalpolicy_binding

Binding object showing the authenticationlocalpolicy that can be bound to authenticationvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
policy	<String>	Read-write	The name of the policy, if any, bound to the authentication vserver.
gotopriorityexpression	<String>	Read-write	Applicable only to advance authentication policy. Expression or other value specifying the next policy to be evaluated if the current policy evaluates to TRUE. Specify one of the following values: * NEXT - Evaluate the policy with the next higher priority number. * END - End policy evaluation. * USE_INVOCATION_RESULT - Applicable if this policy invokes another policy label. If the final goto in the invoked policy label has a value of END, the evaluation stops. If the final goto is anything other than END, the current policy label performs a NEXT. * An expression that evaluates to a number. If you specify an

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			expression, the number to which it evaluates determines the next policy to evaluate, as follows: * If the expression evaluates to a higher numbered priority, the policy with that priority is evaluated next. * If the expression evaluates to the priority of the current policy, the policy with the next higher numbered priority is evaluated next. * If the expression evaluates to a priority number that is numerically higher than the highest numbered priority, policy evaluation ends. An UNDEF event is triggered if: * The expression is invalid. * The expression evaluates to a priority number that is numerically lower than the current policy's priority. * The expression evaluates to a priority number that is between the current policy's priority number (say, 30) and the highest

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			priority number (say, 100), but does not match any configured priority number (for example, the expression evaluates to the number 85). This example assumes that the priority number increments by 10 for every successive policy, and therefore a priority number of 85 does not exist in the policy label.
nextfactor	<String>	Read-write	Applicable only while binding advance authentication policy as classic authentication policy does not support nFactor.
groupextraction	<Boolean>	Read-write	Applicable only while bindind classic authentication policy as advance authentication policy use nFactor.
priority	<Integer>	Read-write	The priority, if any, of the vpn vserver policy.
bindpoint	<String>	Read-write	Bind point to which to bind the policy. Applies only to rewrite and cache

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			policies. If you do not set this parameter, the policy is bound to REQ_DEFAULT or RES_DEFAULT, depending on whether the policy rule is a response-time or a request-time expression. Possible values = REQUEST, RESPONSE, ICA_REQUEST, OTHERTCP_REQUEST, AAA_REQUEST, AAA_RESPONSE
secondary	<Boolean>	Read-write	Bind the authentication policy to the secondary chain. Provides for multifactor authentication in which a user must authenticate via both a primary authentication method and, afterward, via a secondary authentication method. Because user groups are aggregated across authentication systems, usernames must be the same on all authentication

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			servers. Passwords can be different.
name	<String>	Read-write	Name of the authentication virtual server to which to bind the policy. Minimum length = 1
acttype	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.
- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/ authenticationvserver_authenticationlocalpolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"authenticationvserver_authenticationlocalpolicy_binding":{

<b>"name":<String_value>,

</b>"policy":<String_value>,

"priority":<Integer_value>,

"secondary":<Boolean_value>,

"groupextraction":<Boolean_value>,

"nextfactor":<String_value>,

"gotopriorityexpression":<String_value>,

"bindpoint":<String_value>
```

```
}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_authenticationlocalpolicy_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_authenticationlocalpolicy_binding/ name_value<String> ? **args=policy: <String_value> ,secondary: <Boolean_value> ,groupextraction: <Boolean_value> ,bindpoint: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_authenticationlocalpolicy_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_authenticationlocalpolicy_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of authenticationvserver_authenticationlocalpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_authenticationlocalpolicy_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authenticationvserver_authenticationlocalpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationvserver_authenticationlocalpolicy_binding": [ {

"policy":<String_value>,

"gotopriorityexpression":<String_value>,

"nextfactor":<String_value>,

"groupextraction":<Boolean_value>,

"priority":<Integer_value>,

"bindpoint":<String_value>,

"secondary":<Boolean_value>,

"name":<String_value>,

"acttype":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_authenticationlocalpolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_authenticationlocalpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationvserver_authenticationlocalpolicy_binding": [ {

"policy":<String_value>,

"gotopriorityexpression":<String_value>,

"nextfactor":<String_value>,

"groupextraction":<Boolean_value>,

"priority":<Integer_value>,

"bindpoint":<String_value>,
```

```
"secondary":<Boolean_value>,

"name":<String_value>,

"acttype":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_authenticationlocalpolicy_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"authenticationvserver_authenticationlocalpolicy_binding": [ { "__count":
"#no"} ] }
```

authenticationvserver_authenticationloginschemapolicy_binding

Binding object showing the authenticationloginschemapolicy that can be bound to authenticationvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
groupextraction	<Boolean>	Read-write	Applicable only while bindind classic authentication policy as advance authentication policy use nFactor.
nextfactor	<String>	Read-write	Applicable only while binding advance authentication policy as classic authentication policy does not support nFactor.
gotopriorityexpression	<String>	Read-write	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
policy	<String>	Read-write	The name of the policy, if any, bound to the authentication vserver.
name	<String>	Read-write	Name of the authentication virtual server to which to bind the policy. Minimum length = 1
secondary	<Boolean>	Read-write	Applicable only while bindind classic authentication policy as advance authentication policy use nFactor.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
bindpoint	<String>	Read-write	Bind point to which to bind the policy. Applies only to rewrite and cache policies. If you do not set this parameter, the policy is bound to REQ_DEFAULT or RES_DEFAULT, depending on whether the policy rule is a response-time or a request-time expression. Possible values = REQUEST, RESPONSE, ICA_REQUEST, OTHERTCP_REQUEST, AAA_REQUEST, AAA_RESPONSE
priority	<Integer>	Read-write	The priority, if any, of the vpn vserver policy.
acttype	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)

- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/authenticationvserver_authenticationloginschemapolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"authenticationvserver_authenticationloginschemapolicy_binding":{

<b>"name":<String_value>,

</b>"policy":<String_value>,

"priority":<Integer_value>,

"secondary":<Boolean_value>,

"groupextraction":<Boolean_value>,

"nextfactor":<String_value>,

"gotopriorityexpression":<String_value>,

"bindpoint":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_authenticationloginschemapolicy_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_authenticationloginschemapolicy_binding/ name_value<String> ? **args=policy: <String_value> ,secondary: <Boolean_value> ,groupextraction: <Boolean_value> ,bindpoint: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_authenticationloginschemapolicy_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_authenticationloginschemapolicy_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of authenticationvserver_authenticationloginschemapolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_authenticationloginschemapolicy_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authenticationvserver_authenticationloginschemapolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationvserver_authenticationloginschemapolicy_binding": [ {

"groupextraction":<Boolean_value>,

"nextfactor":<String_value>,

"gotopriorityexpression":<String_value>,

"policy":<String_value>,

"name":<String_value>,

"secondary":<Boolean_value>,

"bindpoint":<String_value>,

"priority":<Integer_value>,

"acttype":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_authenticationloginschemapolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_authenticationloginschemapolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationvserver_authenticationloginschemapolicy_binding": [ {

"groupextraction":<Boolean_value>,

"nextfactor":<String_value>,

"gotopriorityexpression":<String_value>,

"policy":<String_value>,

"name":<String_value>,

"secondary":<Boolean_value>,

"bindpoint":<String_value>,

"priority":<Integer_value>,

"acttype":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_authenticationloginschemapolicy_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"authenticationvserver_authenticationloginschemapolicy_binding":
[ { "__count": "#no"} ] }
```

authenticationvserver_authenticationnegotiatepolicy_binding

Binding object showing the authenticationnegotiatepolicy that can be bound to authenticationvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
gotopriorityexpression	<String>	Read-write	Applicable only to advance authentication policy. Expression or other value specifying the next policy to be evaluated if the current policy evaluates to TRUE. Specify one of the following values: * NEXT - Evaluate the policy with the next higher priority number. * END - End policy evaluation. * USE_INVOCATION_RESULT - Applicable

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			if this policy invokes another policy label. If the final goto in the invoked policy label has a value of END, the evaluation stops. If the final goto is anything other than END, the current policy label performs a NEXT. * An expression that evaluates to a number. If you specify an expression, the number to which it evaluates determines the next policy to evaluate, as follows: * If the expression evaluates to a higher numbered priority, the policy with that priority is evaluated next. * If the expression evaluates to the priority of the current policy, the policy with the next higher numbered priority is evaluated next. * If the expression evaluates to a priority number that is numerically higher than the highest numbered priority, policy evaluation ends. An

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			UNDEF event is triggered if: * The expression is invalid. * The expression evaluates to a priority number that is numerically lower than the current policy's priority. * The expression evaluates to a priority number that is between the current policy's priority number (say, 30) and the highest priority number (say, 100), but does not match any configured priority number (for example, the expression evaluates to the number 85). This example assumes that the priority number increments by 10 for every successive policy, and therefore a priority number of 85 does not exist in the policy label.
policy	<String>	Read-write	The name of the policy, if any, bound to the authentication vserver.
groupextraction	<Boolean>	Read-write	Applicable only while bindind classic authentication policy

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			as advance authentication policy use nFactor.
nextfactor	<String>	Read-write	Applicable only while binding advance authentication policy as classic authentication policy does not support nFactor.
name	<String>	Read-write	Name of the authentication virtual server to which to bind the policy. Minimum length = 1
secondary	<Boolean>	Read-write	Bind the authentication policy to the secondary chain. Provides for multifactor authentication in which a user must authenticate via both a primary authentication method and, afterward, via a secondary authentication method. Because user groups are aggregated across authentication systems, usernames must be the same on all authentication servers. Passwords can be different.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
priority	<Integer>	Read-write	The priority, if any, of the vpn vserver policy.
bindpoint	<String>	Read-write	Bind point to which to bind the policy. Applies only to rewrite and cache policies. If you do not set this parameter, the policy is bound to REQ_DEFAULT or RES_DEFAULT, depending on whether the policy rule is a response-time or a request-time expression. Possible values = REQUEST, RESPONSE, ICA_REQUEST, OTHERTCP_REQUEST, AAA_REQUEST, AAA_RESPONSE
acttype	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)

- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/authenticationvserver_authenticationnegotiatepolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"authenticationvserver_authenticationnegotiatepolicy_binding":{

<b>"name":<String_value>,

</b>"policy":<String_value>,

"priority":<Integer_value>,

"secondary":<Boolean_value>,

"groupextraction":<Boolean_value>,

"nextfactor":<String_value>,

"gotopriorityexpression":<String_value>,

"bindpoint":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_authenticationnegotiatepolicy_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_authenticationnegotiatepolicy_binding/ name_value<String> ? **args=policy: <String_value> ,secondary: <Boolean_value> ,groupextraction: <Boolean_value> ,bindpoint: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_authenticationnegotiatepolicy_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_authenticationnegotiatepolicy_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of authenticationvserver_authenticationnegotiatepolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_authenticationnegotiatepolicy_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authenticationvserver_authenticationnegotiatepolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationvserver_authenticationnegotiatepolicy_binding": [ {

"gotopriorityexpression":<String_value>,

"policy":<String_value>,

"groupextraction":<Boolean_value>,

"nextfactor":<String_value>,

"name":<String_value>,

"secondary":<Boolean_value>,

"priority":<Integer_value>,

"bindpoint":<String_value>,

"acttype":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_authenticationnegotiatepolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_authenticationnegotiatepolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationvserver_authenticationnegotiatepolicy_binding": [ {

"gotopriorityexpression":<String_value>,

"policy":<String_value>,

"groupextraction":<Boolean_value>,

"nextfactor":<String_value>,

"name":<String_value>,

"secondary":<Boolean_value>,

"priority":<Integer_value>,

"bindpoint":<String_value>,

"acttype":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_authenticationnegotiatepolicy_binding/ name_value<String> ? **count=yes**
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"authenticationvserver_authenticationnegotiatepolicy_binding":
[ { "__count": "#no"} ] }
```

authenticationvserver_authenticationoauthidppolicy_binding

Binding object showing the authenticationoauthidppolicy that can be bound to authenticationvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
groupextraction	<Boolean>	Read-write	Applicable only while bindind classic authentication policy as advance authentication policy use nFactor.
nextfactor	<String>	Read-write	On success invoke label.
gotopriorityexpression	<String>	Read-write	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
policy	<String>	Read-write	The name of the policy, if any, bound to the authentication vserver.
name	<String>	Read-write	Name of the authentication virtual server to which to bind the policy. Minimum length = 1
secondary	<Boolean>	Read-write	Applicable only while bindind classic authentication policy as advance authentication policy use nFactor.
bindpoint	<String>	Read-write	Bind point to which to bind the policy. Applies only to rewrite and cache policies. If you do not set this parameter, the policy is bound to REQ_DEFAULT or RES_DEFAULT, depending on whether the policy rule is a response-time or a request-time expression. Possible values = REQUEST, RESPONSE, ICA_REQUEST, OTHERTCP_REQUEST,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			AAA_REQUEST, AAA_RESPONSE
priority	<Integer>	Read-write	The priority, if any, of the vpn vserver policy.
acttype	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/ authenticationvserver_authenticationoauthidppolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"authenticationvserver_authenticationoauthidppolicy_binding":{

<b>"name":<String_value>,

</b>"policy":<String_value>,

"priority":<Integer_value>,

"secondary":<Boolean_value>,

"groupextraction":<Boolean_value>,

"nextfactor":<String_value>,

"gotopriorityexpression":<String_value>,

"bindpoint":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_authenticationoauthidppolicy_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_authenticationoauthidppolicy_binding/ name_value<String> ? **args=policy: <String_value> ,secondary: <Boolean_value> ,groupextraction: <Boolean_value> ,bindpoint: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_authenticationoauthidppolicy_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_authenticationoauthidppolicy_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of authenticationvserver_authenticationoauthidppolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_authenticationoauthidppolicy_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authenticationvserver_authenticationoauthidppolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationvserver_authenticationoauthidppolicy_binding": [ {

"groupextraction":<Boolean_value>,

"nextfactor":<String_value>,

"gotopriorityexpression":<String_value>,

"policy":<String_value>,

"name":<String_value>,

"secondary":<Boolean_value>,

"bindpoint":<String_value>,

"priority":<Integer_value>,

"acttype":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_authenticationoauthidppolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_authenticationoauthidppolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationvserver_authenticationoauthidppolicy_binding": [ {

"groupextraction":<Boolean_value>,

"nextfactor":<String_value>,

"gotopriorityexpression":<String_value>,

"policy":<String_value>,

"name":<String_value>,

"secondary":<Boolean_value>,
```

```
"bindpoint":<String_value>,

"priority":<Integer_value>,

"acttype":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_authenticationoauthidppolicy_binding/ name_value<String> ? **count=yes**
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"authenticationvserver_authenticationoauthidppolicy_binding":
[ { "__count": "#no"} ] }
```

authenticationvserver_authenticationpolicy_binding

Binding object showing the authenticationpolicy that can be bound to authenticationvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
priority	<Integer>	Read-write	The priority, if any, of the vpn vserver policy.
bindpoint	<String>	Read-write	Bind point to which to bind the policy. Applies only to rewrite and cache policies. If you do not set this parameter, the policy is bound to REQ_DEFAULT or RES_DEFAULT, depending on whether the policy rule is a response-time or a request-time expression. Possible values = REQUEST, RESPONSE, ICA_REQUEST, OTHERTCP_REQUEST, AAA_REQUEST, AAA_RESPONSE
secondary	<Boolean>	Read-write	Applicable only while bindind classic authentication policy as advance authentication policy use nFactor.
name	<String>	Read-write	Name of the authentication virtual server to which to bind the policy. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
policy	<String>	Read-write	The name of the policy, if any, bound to the authentication vserver.
gotopriorityexpression	<String>	Read-write	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
nextfactor	<String>	Read-write	On success invoke label.
groupextraction	<Boolean>	Read-write	Applicable only while bindind classic authentication policy as advance authentication policy use nFactor.
acttype	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/ authenticationvserver_authenticationpolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"authenticationvserver_authenticationpolicy_binding":{

<b>"name":<String_value>,
```

```
</b>"policy":<String_value>,

"priority":<Integer_value>,

"secondary":<Boolean_value>,

"groupextraction":<Boolean_value>,

"nextfactor":<String_value>,

"gotopriorityexpression":<String_value>,

"bindpoint":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_authenticationpolicy_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_authenticationpolicy_binding/ name_value<String> ? **args=policy: <String_value> ,secondary: <Boolean_value> ,groupextraction: <Boolean_value> ,bindpoint: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_authenticationpolicy_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_authenticationpolicy_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of authenticationvserver_authenticationpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_authenticationpolicy_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authenticationvserver_authenticationpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationvserver_authenticationpolicy_binding": [ {

"priority":<Integer_value>,

"bindpoint":<String_value>,
```

```
"secondary":<Boolean_value>,

"name":<String_value>,

"policy":<String_value>,

"gotopriorityexpression":<String_value>,

"nextfactor":<String_value>,

"groupextraction":<Boolean_value>,

"acttype":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_authenticationpolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_authenticationpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationvserver_authenticationpolicy_binding": [ {

"priority":<Integer_value>,

"bindpoint":<String_value>,

"secondary":<Boolean_value>,

"name":<String_value>,

"policy":<String_value>,

"gotopriorityexpression":<String_value>,

"nextfactor":<String_value>,

"groupextraction":<Boolean_value>,

"acttype":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_authenticationpolicy_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"authenticationvserver_authenticationpolicy_binding": [ { "__count":
"#no"} ] }
```

authenticationvserver_authenticationradiuspolicy_binding

Binding object showing the authenticationradiuspolicy that can be bound to authenticationvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
policy	<String>	Read-write	The name of the policy, if any, bound to the authentication vserver.
gotopriorityexpression	<String>	Read-write	Applicable only to advance authentication policy. Expression or other value specifying the next policy to be evaluated if the current policy evaluates to TRUE. Specify one of the following values: * NEXT - Evaluate the policy with the next higher priority number. * END - End policy evaluation. * USE_INVOCATION_RESULT - Applicable if this policy invokes another policy label. If the final goto in the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			invoked policy label has a value of END, the evaluation stops. If the final goto is anything other than END, the current policy label performs a NEXT. * An expression that evaluates to a number. If you specify an expression, the number to which it evaluates determines the next policy to evaluate, as follows: * If the expression evaluates to a higher numbered priority, the policy with that priority is evaluated next. * If the expression evaluates to the priority of the current policy, the policy with the next higher numbered priority is evaluated next. * If the expression evaluates to a priority number that is numerically higher than the highest numbered priority, policy evaluation ends. An UNDEF event is triggered if: * The expression is invalid.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			* The expression evaluates to a priority number that is numerically lower than the current policy's priority. * The expression evaluates to a priority number that is between the current policy's priority number (say, 30) and the highest priority number (say, 100), but does not match any configured priority number (for example, the expression evaluates to the number 85). This example assumes that the priority number increments by 10 for every successive policy, and therefore a priority number of 85 does not exist in the policy label.
groupextraction	<Boolean>	Read-write	Applicable only while bindind classic authentication policy as advance authentication policy use nFactor.
nextfactor	<String>	Read-write	Applicable only while binding advance authentication policy as classic

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			authentication policy does not support nFactor.
secondary	<Boolean>	Read-write	Bind the authentication policy to the secondary chain. Provides for multifactor authentication in which a user must authenticate via both a primary authentication method and, afterward, via a secondary authentication method. Because user groups are aggregated across authentication systems, usernames must be the same on all authentication servers. Passwords can be different.
name	<String>	Read-write	Name of the authentication virtual server to which to bind the policy. Minimum length = 1
bindpoint	<String>	Read-write	Bind point to which to bind the policy. Applies only to rewrite and cache policies. If you do not set this parameter, the policy is bound to

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			REQ_DEFAULT or RES_DEFAULT, depending on whether the policy rule is a response-time or a request-time expression. Possible values = REQUEST, RESPONSE, ICA_REQUEST, OTHERTCP_REQUEST, AAA_REQUEST, AAA_RESPONSE
priority	<Integer>	Read-write	The priority, if any, of the vpn vserver policy.
acttype	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/authenticationvserver_authenticationradiuspolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"authenticationvserver_authenticationradiuspolicy_binding":{

<b>"name":<String_value>,

</b>"policy":<String_value>,

"priority":<Integer_value>,
```

```
"secondary":<Boolean_value>,

"groupextraction":<Boolean_value>,

"nextfactor":<String_value>,

"gotopriorityexpression":<String_value>,

"bindpoint":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_authenticationradiuspolicy_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_authenticationradiuspolicy_binding/ name_value<String> ? **args=policy: <String_value> ,secondary: <Boolean_value> ,groupextraction: <Boolean_value> ,bindpoint: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_authenticationradiuspolicy_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/

authenticationvserver_authenticationradiuspolicy_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of authenticationvserver_authenticationradiuspolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_authenticationradiuspolicy_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authenticationvserver_authenticationradiuspolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationvserver_authenticationradiuspolicy_binding": [ {

"policy":<String_value>,

"gotopriorityexpression":<String_value>,

"groupextraction":<Boolean_value>,

"nextfactor":<String_value>,

"secondary":<Boolean_value>,
```

```
"name":<String_value>,

"bindpoint":<String_value>,

"priority":<Integer_value>,

"acttype":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_authenticationradiuspolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_authenticationradiuspolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationvserver_authenticationradiuspolicy_binding": [ {

"policy":<String_value>,
```

```
"gotopriorityexpression":<String_value>,

"groupextraction":<Boolean_value>,

"nextfactor":<String_value>,

"secondary":<Boolean_value>,

"name":<String_value>,

"bindpoint":<String_value>,

"priority":<Integer_value>,

"acttype":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_authenticationradiuspolicy_binding/ name_value<String> ? **count=yes**
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"authenticationvserver_authenticationradiuspolicy_binding":
[ { "__count": "#no"} ] }
```

authenticationvserver_authenticationsamlidppolicy_binding

Binding object showing the authenticationsamlidppolicy that can be bound to authenticationvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
gotopriorityexpression	<String>	Read-write	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
policy	<String>	Read-write	The name of the policy, if any, bound to the authentication vserver.
nextfactor	<String>	Read-write	On success invoke label.
groupextraction	<Boolean>	Read-write	Applicable only while bindind classic authentication policy as advance authentication policy use nFactor.
bindpoint	<String>	Read-write	Bind point to which to bind the policy. Applies only to rewrite and cache policies. If you do not set this parameter,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			the policy is bound to REQ_DEFAULT or RES_DEFAULT, depending on whether the policy rule is a response-time or a request-time expression. Possible values = REQUEST, RESPONSE, ICA_REQUEST, OTHERTCP_REQUEST, AAA_REQUEST, AAA_RESPONSE
priority	<Integer>	Read-write	The priority, if any, of the vpn vserver policy.
name	<String>	Read-write	Name of the authentication virtual server to which to bind the policy. Minimum length = 1
secondary	<Boolean>	Read-write	Applicable only while bindind classic authentication policy as advance authentication policy use nFactor.
acttype	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/authenticationvserver_authenticationsamlidppolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"authenticationvserver_authenticationsamlidppolicy_binding":{

<b>"name":<String_value>,

</b>"policy":<String_value>,

"priority":<Integer_value>,

"secondary":<Boolean_value>,

"groupextraction":<Boolean_value>,

"nextfactor":<String_value>,

"gotopriorityexpression":<String_value>,

"bindpoint":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_authenticationsamlidppolicy_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_authenticationsamlidppolicy_binding/ name_value<String> ? **args=policy: <String_value> ,secondary: <Boolean_value> ,groupextraction: <Boolean_value> ,bindpoint: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_authenticationsamlidppolicy_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_authenticationsamlidppolicy_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of authenticationvserver_authenticationsamlidppolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_authenticationsamlidppolicy_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authenticationvserver_authenticationsamlidppolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationvserver_authenticationsamlidppolicy_binding": [ {

"gotopriorityexpression":<String_value>,

"policy":<String_value>,

"nextfactor":<String_value>,

"groupextraction":<Boolean_value>,

"bindpoint":<String_value>,

"priority":<Integer_value>,

"name":<String_value>,

"secondary":<Boolean_value>,

"acttype":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_authenticationsamlidppolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_authenticationsamlidppolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationvserver_authenticationsamlidppolicy_binding": [ {

"gotopriorityexpression":<String_value>,

"policy":<String_value>,

"nextfactor":<String_value>,

"groupextraction":<Boolean_value>,

"bindpoint":<String_value>,

"priority":<Integer_value>,

"name":<String_value>,

"secondary":<Boolean_value>,

"acttype":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_authenticationsamlidppolicy_binding/ name_value<String> ? **count=yes**
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"authenticationvserver_authenticationsamlidppolicy_binding":
[ { "__count": "#no"} ] }
```

authenticationvserver_authenticationsamlpolicy_binding

Binding object showing the authenticationsamlpolicy that can be bound to authenticationvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
groupextraction	<Boolean>	Read-write	Applicable only while bindind classic authentication policy as advance authentication policy use nFactor.
nextfactor	<String>	Read-write	Applicable only while binding advance authentication policy as classic authentication policy does not support nFactor.
policy	<String>	Read-write	The name of the policy, if any, bound

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			to the authentication vserver.
gotopriorityexpression	<String>	Read-write	Applicable only to advance authentication policy. Expression or other value specifying the next policy to be evaluated if the current policy evaluates to TRUE. Specify one of the following values: * NEXT - Evaluate the policy with the next higher priority number. * END - End policy evaluation. * USE_INVOCATION_RESULT - Applicable if this policy invokes another policy label. If the final goto in the invoked policy label has a value of END, the evaluation stops. If the final goto is anything other than END, the current policy label performs a NEXT. * An expression that evaluates to a number. If you specify an expression, the number to which it evaluates determines the next policy to evaluate, as

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			follows: * If the expression evaluates to a higher numbered priority, the policy with that priority is evaluated next. * If the expression evaluates to the priority of the current policy, the policy with the next higher numbered priority is evaluated next. * If the expression evaluates to a priority number that is numerically higher than the highest numbered priority, policy evaluation ends. An UNDEF event is triggered if: * The expression is invalid. * The expression evaluates to a priority number that is numerically lower than the current policy's priority. * The expression evaluates to a priority number that is between the current policy's priority number (say, 30) and the highest priority number (say, 100), but does not match any configured priority number (for

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			example, the expression evaluates to the number 85). This example assumes that the priority number increments by 10 for every successive policy, and therefore a priority number of 85 does not exist in the policy label.
secondary	<Boolean>	Read-write	Bind the authentication policy to the secondary chain. Provides for multifactor authentication in which a user must authenticate via both a primary authentication method and, afterward, via a secondary authentication method. Because user groups are aggregated across authentication systems, usernames must be the same on all authentication servers. Passwords can be different.
name	<String>	Read-write	Name of the authentication virtual server to which to bind the policy.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum length = 1
priority	<Integer>	Read-write	The priority, if any, of the vpn vserver policy.
bindpoint	<String>	Read-write	Bind point to which to bind the policy. Applies only to rewrite and cache policies. If you do not set this parameter, the policy is bound to REQ_DEFAULT or RES_DEFAULT, depending on whether the policy rule is a response-time or a request-time expression. Possible values = REQUEST, RESPONSE, ICA_REQUEST, OTHERTCP_REQUEST, AAA_REQUEST, AAA_RESPONSE
acttype	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET

- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/authenticationvserver_authenticationsamlpolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"authenticationvserver_authenticationsamlpolicy_binding":{

<b>"name":<String_value>,

</b>"policy":<String_value>,

"priority":<Integer_value>,

"secondary":<Boolean_value>,

"groupextraction":<Boolean_value>,

"nextfactor":<String_value>,

"gotopriorityexpression":<String_value>,

"bindpoint":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_authenticationsamlpolicy_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_authenticationsamlpolicy_binding/ name_value<String> ? **args=policy: <String_value> ,secondary: <Boolean_value> ,groupextraction: <Boolean_value> ,bindpoint: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_authenticationsamlpolicy_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_authenticationsamlpolicy_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of authenticationvserver_authenticationsamlpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_authenticationsamlpolicy_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authenticationvserver_authenticationsamlpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationvserver_authenticationsamlpolicy_binding": [ {

"groupextraction":<Boolean_value>,

"nextfactor":<String_value>,

"policy":<String_value>,

"gotopriorityexpression":<String_value>,

"secondary":<Boolean_value>,

"name":<String_value>,

"priority":<Integer_value>,

"bindpoint":<String_value>,

"acttype":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_authenticationsamlpolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_authenticationsamlpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationvserver_authenticationsamlpolicy_binding": [ {

"groupextraction":<Boolean_value>,

"nextfactor":<String_value>,

"policy":<String_value>,

"gotopriorityexpression":<String_value>,

"secondary":<Boolean_value>,

"name":<String_value>,

"priority":<Integer_value>,

"bindpoint":<String_value>,

"acttype":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_authenticationsamlpolicy_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"authenticationvserver_authenticationsamlpolicy_binding": [ { "__count":
"#no"} ] }
```

authenticationvserver_authenticationsmartaccesspolicy_binding

Binding object showing the authenticationsmartaccesspolicy that can be bound to authenticationvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
bindpoint	<String>	Read-write	Bind point to which to bind the policy. Applies only to rewrite and cache policies. If you do not set this parameter, the policy is bound to REQ_DEFAULT or RES_DEFAULT, depending on whether the policy rule is a response-time or a request-time expression. Possible values = REQUEST, RESPONSE,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			ICA_REQUEST, OTHERTCP_REQUEST, AAA_REQUEST, AAA_RESPONSE
priority	<Integer>	Read-write	The priority, if any, of the vpn vserver policy.
secondary	<Boolean>	Read-write	Applicable only while bindind classic authentication policy as advance authentication policy use nFactor.
name	<String>	Read-write	Name of the authentication virtual server to which to bind the policy. Minimum length = 1
policy	<String>	Read-write	The name of the policy, if any, bound to the authentication vserver.
gotopriorityexpression	<String>	Read-write	Applicable only to advance authentication policy. Expression or other value specifying the next policy to be evaluated if the current policy evaluates to TRUE. Specify one of the following values: * NEXT - Evaluate the policy with the next

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			higher priority number. * END - End policy evaluation. * USE_INVOCATION_RESULT - Applicable if this policy invokes another policy label. If the final goto in the invoked policy label has a value of END, the evaluation stops. If the final goto is anything other than END, the current policy label performs a NEXT. * An expression that evaluates to a number. If you specify an expression, the number to which it evaluates determines the next policy to evaluate, as follows: * If the expression evaluates to a higher numbered priority, the policy with that priority is evaluated next. * If the expression evaluates to the priority of the current policy, the policy with the next higher numbered priority is evaluated next. * If the expression evaluates to a priority number

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			that is numerically higher than the highest numbered priority, policy evaluation ends. An UNDEF event is triggered if: * The expression is invalid. * The expression evaluates to a priority number that is numerically lower than the current policy's priority. * The expression evaluates to a priority number that is between the current policy's priority number (say, 30) and the highest priority number (say, 100), but does not match any configured priority number (for example, the expression evaluates to the number 85). This example assumes that the priority number increments by 10 for every successive policy, and therefore a priority number of 85 does not exist in the policy label.
nextfactor	<String>	Read-write	Applicable only while binding advance authentication policy

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			as classic authentication policy does not support nFactor.
groupextraction	<Boolean>	Read-write	Applicable only while bindind classic authentication policy as advance authentication policy use nFactor.
acttype	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of

creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/ authenticationvserver_authenticationsmartaccesspolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"authenticationvserver_authenticationsmartaccesspolicy_binding":{

<b>"name":<String_value>,

</b>"policy":<String_value>,

"priority":<Integer_value>,

"secondary":<Boolean_value>,

"groupextraction":<Boolean_value>,

"nextfactor":<String_value>,
```

```
"gotopriorityexpression":<String_value>,

"bindpoint":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_authenticationsmartaccesspolicy_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_authenticationsmartaccesspolicy_binding/ name_value<String> ? **args=policy: <String_value> ,secondary: <Boolean_value> ,groupextraction: <Boolean_value> ,bindpoint: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_authenticationsmartaccesspolicy_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_authenticationsmartaccesspolicy_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of authenticationvserver_authenticationsmartaccesspolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_authenticationsmartaccesspolicy_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authenticationvserver_authenticationsmartaccesspolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationvserver_authenticationsmartaccesspolicy_binding": [ {

"bindpoint":<String_value>,

"priority":<Integer_value>,

"secondary":<Boolean_value>,

"name":<String_value>,

"policy":<String_value>,

"gotopriorityexpression":<String_value>,

"nextfactor":<String_value>,

"groupextraction":<Boolean_value>,
```

```
"acttype":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_authenticationsmartaccesspolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_authenticationsmartaccesspolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationvserver_authenticationsmartaccesspolicy_binding": [ {

"bindpoint":<String_value>,

"priority":<Integer_value>,

"secondary":<Boolean_value>,

"name":<String_value>,
```

```
"policy":<String_value>,

"gotopriorityexpression":<String_value>,

"nextfactor":<String_value>,

"groupextraction":<Boolean_value>,

"acttype":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_authenticationsmartaccesspolicy_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"authenticationvserver_authenticationsmartaccesspolicy_binding":
[ { "__count": "#no"} ] }
```

authenticationvserver_authenticationtacacspolicy_binding

Binding object showing the authenticationtacacspolicy that can be bound to authenticationvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
bindpoint	<String>	Read-write	Bind point to which to bind the policy. Applies only to rewrite and cache policies. If you do not set this parameter, the policy is bound to REQ_DEFAULT or RES_DEFAULT, depending on whether the policy rule is a response-time or a request-time expression. Possible values = REQUEST, RESPONSE, ICA_REQUEST, OTHERTCP_REQUEST, AAA_REQUEST, AAA_RESPONSE
priority	<Integer>	Read-write	The priority, if any, of the vpn vserver policy.
secondary	<Boolean>	Read-write	Bind the authentication policy to the secondary chain. Provides for multifactor authentication in which a user must authenticate via both a primary authentication

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			method and, afterward, via a secondary authentication method. Because user groups are aggregated across authentication systems, usernames must be the same on all authentication servers. Passwords can be different.
name	<String>	Read-write	Name of the authentication virtual server to which to bind the policy. Minimum length = 1
policy	<String>	Read-write	The name of the policy, if any, bound to the authentication vserver.
gotopriorityexpression	<String>	Read-write	Applicable only to advance authentication policy. Expression or other value specifying the next policy to be evaluated if the current policy evaluates to TRUE. Specify one of the following values: * NEXT - Evaluate the policy with the next higher priority number. * END - End policy evaluation. *

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			USE_INVOCATION_RESULT - Applicable if this policy invokes another policy label. If the final goto in the invoked policy label has a value of END, the evaluation stops. If the final goto is anything other than END, the current policy label performs a NEXT. * An expression that evaluates to a number. If you specify an expression, the number to which it evaluates determines the next policy to evaluate, as follows: * If the expression evaluates to a higher numbered priority, the policy with that priority is evaluated next. * If the expression evaluates to the priority of the current policy, the policy with the next higher numbered priority is evaluated next. * If the expression evaluates to a priority number that is numerically higher than the highest numbered

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			priority, policy evaluation ends. An UNDEF event is triggered if: * The expression is invalid. * The expression evaluates to a priority number that is numerically lower than the current policy's priority. * The expression evaluates to a priority number that is between the current policy's priority number (say, 30) and the highest priority number (say, 100), but does not match any configured priority number (for example, the expression evaluates to the number 85). This example assumes that the priority number increments by 10 for every successive policy, and therefore a priority number of 85 does not exist in the policy label.
nextfactor	<String>	Read-write	Applicable only while binding advance authentication policy as classic authentication policy

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			does not support nFactor.
groupextraction	<Boolean>	Read-write	Applicable only while bindind classic authentication policy as advance authentication policy use nFactor.
acttype	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/ authenticationvserver_authenticationtacacspolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"authenticationvserver_authenticationtacacspolicy_binding":{

<b>"name":<String_value>,

</b>"policy":<String_value>,

"priority":<Integer_value>,

"secondary":<Boolean_value>,

"groupextraction":<Boolean_value>,

"nextfactor":<String_value>,

"gotopriorityexpression":<String_value>,

"bindpoint":<String_value>
```

```
}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_authenticationtacacspolicy_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_authenticationtacacspolicy_binding/ name_value<String> ? **args=policy: <String_value> ,secondary: <Boolean_value> ,groupextraction: <Boolean_value> ,bindpoint: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_authenticationtacacspolicy_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_authenticationtacacspolicy_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of authenticationvserver_authenticationtacacspolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_authenticationtacacspolicy_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authenticationvserver_authenticationtacacspolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationvserver_authenticationtacacspolicy_binding": [ {

"bindpoint":<String_value>,

"priority":<Integer_value>,

"secondary":<Boolean_value>,

"name":<String_value>,

"policy":<String_value>,

"gotopriorityexpression":<String_value>,

"nextfactor":<String_value>,

"groupextraction":<Boolean_value>,

"acttype":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_authenticationtacacspolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_authenticationtacacspolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationvserver_authenticationtacacspolicy_binding": [ {

"bindpoint":<String_value>,

"priority":<Integer_value>,

"secondary":<Boolean_value>,

"name":<String_value>,

"policy":<String_value>,

"gotopriorityexpression":<String_value>,
```

```
"nextfactor":<String_value>,

"groupextraction":<Boolean_value>,

"acttype":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_authenticationtacacspolicy_binding/ name_value<String> ? **count=yes**
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"authenticationvserver_authenticationtacacspolicy_binding":
[ { "__count": "#no"} ] }
```

authenticationvserver_authenticationwebauthpolicy_binding

Binding object showing the authenticationwebauthpolicy that can be bound to authenticationvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
bindpoint	<String>	Read-write	Bind point to which to bind the policy. Applies only to rewrite and cache policies. If you do not set this parameter, the policy is bound to REQ_DEFAULT or RES_DEFAULT, depending on whether the policy rule is a response-time or a request-time expression. Possible values = REQUEST, RESPONSE, ICA_REQUEST, OTHERTCP_REQUEST, AAA_REQUEST, AAA_RESPONSE
priority	<Integer>	Read-write	The priority, if any, of the vpn vserver policy.
secondary	<Boolean>	Read-write	Bind the authentication policy to the secondary chain. Provides for multifactor authentication in which a user must authenticate via both a primary authentication method and, afterward, via a secondary

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			authentication method. Because user groups are aggregated across authentication systems, usernames must be the same on all authentication servers. Passwords can be different.
name	<String>	Read-write	Name of the authentication virtual server to which to bind the policy. Minimum length = 1
nextfactor	<String>	Read-write	Applicable only while binding advance authentication policy as classic authentication policy does not support nFactor.
groupextraction	<Boolean>	Read-write	Applicable only while bindind classic authentication policy as advance authentication policy use nFactor.
policy	<String>	Read-write	The name of the policy, if any, bound to the authentication vserver.
gotopriorityexpression	<String>	Read-write	Applicable only to advance authentication policy. Expression or other

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			value specifying the next policy to be evaluated if the current policy evaluates to TRUE. Specify one of the following values: * NEXT - Evaluate the policy with the next higher priority number. * END - End policy evaluation. * USE_INVOCATION_RESULT - Applicable if this policy invokes another policy label. If the final goto in the invoked policy label has a value of END, the evaluation stops. If the final goto is anything other than END, the current policy label performs a NEXT. * An expression that evaluates to a number. If you specify an expression, the number to which it evaluates determines the next policy to evaluate, as follows: * If the expression evaluates to a higher numbered priority, the policy with that priority is evaluated next. * If the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			expression evaluates to the priority of the current policy, the policy with the next higher numbered priority is evaluated next. * If the expression evaluates to a priority number that is numerically higher than the highest numbered priority, policy evaluation ends. An UNDEF event is triggered if: * The expression is invalid. * The expression evaluates to a priority number that is numerically lower than the current policy's priority. * The expression evaluates to a priority number that is between the current policy's priority number (say, 30) and the highest priority number (say, 100), but does not match any configured priority number (for example, the expression evaluates to the number 85). This example assumes that the priority number increments by 10 for

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			every successive policy, and therefore a priority number of 85 does not exist in the policy label.
acttype	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/ authenticationvserver_authenticationwebauthpolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"authenticationvserver_authenticationwebauthpolicy_binding":{

<b>"name":<String_value>,

</b>"policy":<String_value>,

"priority":<Integer_value>,

"secondary":<Boolean_value>,

"groupextraction":<Boolean_value>,

"nextfactor":<String_value>,

"gotopriorityexpression":<String_value>,

"bindpoint":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_authenticationwebauthpolicy_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_authenticationwebauthpolicy_binding/ name_value<String> ? **args=policy: <String_value> ,secondary: <Boolean_value> ,groupextraction: <Boolean_value> ,bindpoint: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_authenticationwebauthpolicy_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_authenticationwebauthpolicy_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of authenticationvserver_authenticationwebauthpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_authenticationwebauthpolicy_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authenticationvserver_authenticationwebauthpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationvserver_authenticationwebauthpolicy_binding": [ {

"bindpoint":<String_value>,

"priority":<Integer_value>,

"secondary":<Boolean_value>,

"name":<String_value>,

"nextfactor":<String_value>,

"groupextraction":<Boolean_value>,

"policy":<String_value>,

"gotopriorityexpression":<String_value>,

"acttype":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_authenticationwebauthpolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_authenticationwebauthpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationvserver_authenticationwebauthpolicy_binding": [ {

"bindpoint":<String_value>,

"priority":<Integer_value>,

"secondary":<Boolean_value>,

"name":<String_value>,

"nextfactor":<String_value>,

"groupextraction":<Boolean_value>,

"policy":<String_value>,

"gotopriorityexpression":<String_value>,

"acttype":<Integer_value>
```

```
}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_authenticationwebauthpolicy_binding/ name_value<String> ? **count=yes**
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"authenticationvserver_authenticationwebauthpolicy_binding":
[ { "__count": "#no"} ] }
```

authenticationvserver_binding

Binding object which returns the resources bound to authenticationvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the authentication virtual server.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum length = 1
authenticationvserver_authenticationradiuspolicy_binding	<authenticationvserver_authenticationradiuspolicy_binding[]>	Read-only	authenticationradiuspolicy that can be bound to authenticationvserver.
authenticationvserver_authenticationtacacspolicy_binding	<authenticationvserver_authenticationtacacspolicy_binding[]>	Read-only	authenticationtacacspolicy that can be bound to authenticationvserver.
authenticationvserver_vpnportaltheme_binding	<authenticationvserver_vpnportaltheme_binding[]>	Read-only	vpnportaltheme that can be bound to authenticationvserver.
authenticationvserver_authenticationoauthidppolicy_binding	<authenticationvserver_authenticationoauthidppolicy_binding[]>	Read-only	authenticationoauthidppolicy that can be bound to authenticationvserver.
authenticationvserver_tmsessionpolicy_binding	<authenticationvserver_tmsessionpolicy_binding[]>	Read-only	tmsessionpolicy that can be bound to authenticationvserver.
authenticationvserver_authenticationcertpolicy_binding	<authenticationvserver_authenticationcertpolicy_binding[]>	Read-only	authenticationcertpolicy that can be bound to authenticationvserver.
authenticationvserver_authenticationsmartaccesspolicy_binding	<authenticationvserver_authenticationsmartaccesspolicy_binding[]>	Read-only	authenticationsmartaccesspolicy that can be bound to authenticationvserver.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
authenticationvserver_auditnslogpolicy_binding	<authenticationvserver_auditnslogpolicy_binding[]>	Read-only	auditnslogpolicy that can be bound to authenticationvserver.
authenticationvserver_authenticationpolicy_binding	<authenticationvserver_authenticationpolicy_binding[]>	Read-only	authenticationpolicy that can be bound to authenticationvserver.
authenticationvserver_authenticationsamlpolicy_binding	<authenticationvserver_authenticationsamlpolicy_binding[]>	Read-only	authenticationsamlpolicy that can be bound to authenticationvserver.
authenticationvserver_responderpolicy_binding	<authenticationvserver_responderpolicy_binding[]>	Read-only	responderpolicy that can be bound to authenticationvserver.
authenticationvserver_authenticationnegotiatepolicy_binding	<authenticationvserver_authenticationnegotiatepolicy_binding[]>	Read-only	authenticationnegotiatepolicy that can be bound to authenticationvserver.
authenticationvserver_cspolicy_binding	<authenticationvserver_cspolicy_binding[]>	Read-only	cspolicy that can be bound to authenticationvserver.
authenticationvserver_authenticationsamlidppolicy_binding	<authenticationvserver_authenticationsamlidppolicy_binding[]>	Read-only	authenticationsamlidppolicy that can be bound to authenticationvserver.
authenticationvserver_auditsyslogpolicy_binding	<authenticationvserver_auditsyslogpolicy_binding[]>	Read-only	auditsyslogpolicy that can be bound to

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			authenticationvserver.
authenticationvserver_cachepolicy_binding	<authenticationvserver_cachepolicy_binding[]>	Read-only	cachepolicy that can be bound to authenticationvserver.
authenticationvserver_authenticationloginschemapolicy_binding	<authenticationvserver_authenticationloginschemapolicy_binding[]>	Read-only	authenticationloginschemapolicy that can be bound to authenticationvserver.
authenticationvserver_authenticationlocalpolicy_binding	<authenticationvserver_authenticationlocalpolicy_binding[]>	Read-only	authenticationlocalpolicy that can be bound to authenticationvserver.
authenticationvserver_rewritepolicy_binding	<authenticationvserver_rewritepolicy_binding[]>	Read-only	rewritepolicy that can be bound to authenticationvserver.
authenticationvserver_authenticationldappolicy_binding	<authenticationvserver_authenticationldappolicy_binding[]>	Read-only	authenticationldappolicy that can be bound to authenticationvserver.
authenticationvserver_authenticationwebauthpolicy_binding	<authenticationvserver_authenticationwebauthpolicy_binding[]>	Read-only	authenticationwebauthpolicy that can be bound to authenticationvserver.

Operations

(click to see Properties)

- GET

- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationvserver_binding/name_value<String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationvserver_binding": [ {

"name":<String_value>,

"authenticationvserver_auditsyslogpolicy_binding":<authenticationvserver_a
uditsyslogpolicy_binding[]_value>,

"authenticationvserver_authenticationsmartaccesspolicy_binding":<authentic
ationvserver_authenticationsmartaccesspolicy_binding[]_value>,

"authenticationvserver_responderpolicy_binding":<authenticationvserver_res
ponderpolicy_binding[]_value>,

"authenticationvserver_rewritepolicy_binding":<authenticationvserver_rewri
tepolicy_binding[]_value>,

"authenticationvserver_authenticationradiuspolicy_binding":<authentication
vserver_authenticationradiuspolicy_binding[]_value>,

"authenticationvserver_cachepolicy_binding":<authenticationvserver_cachepo
licy_binding[]_value>,

"authenticationvserver_authenticationloginschemapolicy_binding":<authentic
ationvserver_authenticationloginschemapolicy_binding[]_value>,

"authenticationvserver_authenticationnegotiatepolicy_binding":<authenticat
ionvserver_authenticationnegotiatepolicy_binding[]_value>,

"authenticationvserver_authenticationldappolicy_binding":<authenticationvs
erver_authenticationldappolicy_binding[]_value>,

"authenticationvserver_vpnportaltheme_binding":<authenticationvserver_vpnp
ortaltheme_binding[]_value>,

"authenticationvserver_authenticationcertpolicy_binding":<authenticationvs
erver_authenticationcertpolicy_binding[]_value>,
```

```
"authenticationvserver_auditnslogpolicy_binding":<authenticationvserver_au
ditnslogpolicy_binding[]_value>,

"authenticationvserver_authenticationsamlpolicy_binding":<authenticationvs
erver_authenticationsamlpolicy_binding[]_value>,

"authenticationvserver_tmsessionpolicy_binding":<authenticationvserver_tms
essionpolicy_binding[]_value>,

"authenticationvserver_authenticationlocalpolicy_binding":<authenticationv
server_authenticationlocalpolicy_binding[]_value>,

"authenticationvserver_authenticationpolicy_binding":<authenticationvserve
r_authenticationpolicy_binding[]_value>,

"authenticationvserver_authenticationoauthidppolicy_binding":<authenticati
onvserver_authenticationoauthidppolicy_binding[]_value>,

"authenticationvserver_authenticationsamlidppolicy_binding":<authenticatio
nvserver_authenticationsamlidppolicy_binding[]_value>,

"authenticationvserver_authenticationwebauthpolicy_binding":<authenticatio
nvserver_authenticationwebauthpolicy_binding[]_value>,

"authenticationvserver_cspolicy_binding":<authenticationvserver_cspolicy_b
inding[]_value>,

"authenticationvserver_authenticationtacacspolicy_binding":<authentication
vserver_authenticationtacacspolicy_binding[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationvserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationvserver_binding": [ {

"name":<String_value>,

"authenticationvserver_auditsyslogpolicy_binding":<authenticationvserver_a
uditsyslogpolicy_binding[]_value>,

"authenticationvserver_authenticationsmartaccesspolicy_binding":<authentic
ationvserver_authenticationsmartaccesspolicy_binding[]_value>,

"authenticationvserver_responderpolicy_binding":<authenticationvserver_res
ponderpolicy_binding[]_value>,

"authenticationvserver_rewritepolicy_binding":<authenticationvserver_rewri
tepolicy_binding[]_value>,

"authenticationvserver_authenticationradiuspolicy_binding":<authentication
vserver_authenticationradiuspolicy_binding[]_value>,

"authenticationvserver_cachepolicy_binding":<authenticationvserver_cachepo
licy_binding[]_value>,

"authenticationvserver_authenticationloginschemapolicy_binding":<authentic
ationvserver_authenticationloginschemapolicy_binding[]_value>,

"authenticationvserver_authenticationnegotiatepolicy_binding":<authenticat
```

```
ionvserver_authenticationnegotiatepolicy_binding[]_value>,

"authenticationvserver_authenticationldappolicy_binding":<authenticationvs
erver_authenticationldappolicy_binding[]_value>,

"authenticationvserver_vpnportaltheme_binding":<authenticationvserver_vpnp
ortaltheme_binding[]_value>,

"authenticationvserver_authenticationcertpolicy_binding":<authenticationvs
erver_authenticationcertpolicy_binding[]_value>,

"authenticationvserver_auditnslogpolicy_binding":<authenticationvserver_au
ditnslogpolicy_binding[]_value>,

"authenticationvserver_authenticationsamlpolicy_binding":<authenticationvs
erver_authenticationsamlpolicy_binding[]_value>,

"authenticationvserver_tmsessionpolicy_binding":<authenticationvserver_tms
essionpolicy_binding[]_value>,

"authenticationvserver_authenticationlocalpolicy_binding":<authenticationv
server_authenticationlocalpolicy_binding[]_value>,

"authenticationvserver_authenticationpolicy_binding":<authenticationvserve
r_authenticationpolicy_binding[]_value>,

"authenticationvserver_authenticationoauthidppolicy_binding":<authenticati
onvserver_authenticationoauthidppolicy_binding[]_value>,

"authenticationvserver_authenticationsamlidppolicy_binding":<authenticatio
nvserver_authenticationsamlidppolicy_binding[]_value>,

"authenticationvserver_authenticationwebauthpolicy_binding":<authenticatio
nvserver_authenticationwebauthpolicy_binding[]_value>,

"authenticationvserver_cspolicy_binding":<authenticationvserver_cspolicy_b
inding[]_value>,

"authenticationvserver_authenticationtacacspolicy_binding":<authentication
vserver_authenticationtacacspolicy_binding[]_value>

}]}
```

authenticationvserver_cachepolicy_binding

Binding object showing the cachepolicy that can be bound to authenticationvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
priority	<Integer>	Read-write	The priority, if any, of the vpn vserver policy.
bindpoint	<String>	Read-write	Bindpoint to which the policy is bound. Possible values = REQUEST, RESPONSE, ICA_REQUEST, OTHERTCP_REQUEST, AAA_REQUEST, AAA_RESPONSE
secondary	<Boolean>	Read-write	Applicable only while bindind classic authentication policy as advance authentication policy use nFactor.
name	<String>	Read-write	Name of the authentication virtual server to which to bind the policy. Minimum length = 1
policy	<String>	Read-write	The name of the policy, if any, bound

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			to the authentication vserver.
gotopriorityexpression	<String>	Read-write	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
nextfactor	<String>	Read-write	Applicable only while binding advance authentication policy as classic authentication policy does not support nFactor.
groupextraction	<Boolean>	Read-write	Applicable only while bindind classic authentication policy as advance authentication policy use nFactor.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/authenticationvserver_cachepolicy_binding
HTTP Method: PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"authenticationvserver_cachepolicy_binding":{

<b>"name":<String_value>,
```

```
</b>"policy":<String_value>,

"priority":<Integer_value>,

"secondary":<Boolean_value>,

"groupextraction":<Boolean_value>,

"nextfactor":<String_value>,

"gotopriorityexpression":<String_value>,

"bindpoint":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationvserver_cachepolicy_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_cachepolicy_binding/ name_value<String> ? **args=policy: <String_value> ,secondary: <Boolean_value> ,groupextraction: <Boolean_value> ,bindpoint: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationvserver_cachepolicy_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_cachepolicy_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of authenticationvserver_cachepolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_cachepolicy_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authenticationvserver_cachepolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationvserver_cachepolicy_binding": [ {

"priority":<Integer_value>,

"bindpoint":<String_value>,

"secondary":<Boolean_value>,

"name":<String_value>,
```

```
"policy":<String_value>,

"gotopriorityexpression":<String_value>,

"nextfactor":<String_value>,

"groupextraction":<Boolean_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationvserver_cachepolicy_binding
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/authenticationvserver_cachepolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationvserver_cachepolicy_binding": [ {

"priority":<Integer_value>,
```

```
"bindpoint":<String_value>,

"secondary":<Boolean_value>,

"name":<String_value>,

"policy":<String_value>,

"gotopriorityexpression":<String_value>,

"nextfactor":<String_value>,

"groupextraction":<Boolean_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationvserver_cachepolicy_binding/name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"authenticationvserver_cachepolicy_binding": [ { "__count": "#no"} ] }
```

authenticationvserver_cspolicy_binding

Binding object showing the cspolicy that can be bound to authenticationvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
nextfactor	<String>	Read-write	Applicable only while binding advance authentication policy as classic authentication policy does not support nFactor.
groupextraction	<Boolean>	Read-write	Applicable only while bindind classic authentication policy as advance authentication policy use nFactor.
gotopriorityexpression	<String>	Read-write	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
policy	<String>	Read-write	The name of the policy, if any, bound to the authentication vserver.
priority	<Integer>	Read-write	The priority, if any, of the vpn vserver policy.
bindpoint	<String>	Read-write	Bind point to which to bind the policy. Applies only to

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			rewrite and cache policies. If you do not set this parameter, the policy is bound to REQ_DEFAULT or RES_DEFAULT, depending on whether the policy rule is a response-time or a request-time expression. Possible values = REQUEST, RESPONSE, ICA_REQUEST, OTHERTCP_REQUEST, AAA_REQUEST, AAA_RESPONSE
name	<String>	Read-write	Name of the authentication virtual server to which to bind the policy. Minimum length = 1
secondary	<Boolean>	Read-write	Applicable only while bindind classic authentication policy as advance authentication policy use nFactor.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD

- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/authenticationvserver_cspolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"authenticationvserver_cspolicy_binding":{

<b>"name":<String_value>,

</b>"policy":<String_value>,

"priority":<Integer_value>,

"secondary":<Boolean_value>,

"groupextraction":<Boolean_value>,

"nextfactor":<String_value>,

"gotopriorityexpression":<String_value>,

"bindpoint":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationvserver_cspolicy_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_cspolicy_binding/ name_value<String> ? **args=policy: <String_value> ,secondary: <Boolean_value> ,groupextraction: <Boolean_value> ,bindpoint: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationvserver_cspolicy_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_cspolicy_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of authenticationvserver_cspolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/authenticationvserver_cspolicy_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authenticationvserver_cspolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationvserver_cspolicy_binding": [ {

"nextfactor":<String_value>,

"groupextraction":<Boolean_value>,
```

```
"gotopriorityexpression":<String_value>,

"policy":<String_value>,

"priority":<Integer_value>,

"bindpoint":<String_value>,

"name":<String_value>,

"secondary":<Boolean_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationvserver_cspolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/authenticationvserver_cspolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationvserver_cspolicy_binding": [ {

"nextfactor":<String_value>,

"groupextraction":<Boolean_value>,

"gotopriorityexpression":<String_value>,

"policy":<String_value>,

"priority":<Integer_value>,

"bindpoint":<String_value>,

"name":<String_value>,

"secondary":<Boolean_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationvserver_cspolicy_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"authenticationvserver_cspolicy_binding": [ { "__count": "#no"} ] }
```

authenticationvserver_responderpolicy_binding

Binding object showing the responderpolicy that can be bound to authenticationvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
priority	<Integer>	Read-write	The priority, if any, of the vpn vserver policy.
bindpoint	<String>	Read-write	Bindpoint to which the policy is bound. Possible values = REQUEST, RESPONSE, ICA_REQUEST, OTHERTCP_REQUEST, AAA_REQUEST, AAA_RESPONSE
secondary	<Boolean>	Read-write	Applicable only while bindind classic authentication policy as advance authentication policy use nFactor.
name	<String>	Read-write	Name of the authentication virtual server to which to bind the policy. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
nextfactor	<String>	Read-write	Applicable only while binding advance authentication policy as classic authentication policy does not support nFactor.
groupextraction	<Boolean>	Read-write	Applicable only while bindind classic authentication policy as advance authentication policy use nFactor.
policy	<String>	Read-write	The name of the policy, if any, bound to the authentication vserver.
gotopriorityexpression	<String>	Read-write	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/authenticationvserver_responderpolicy_binding
HTTP Method: PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"authenticationvserver_responderpolicy_binding":{
```

```
<b>"name":<String_value>,

</b>"policy":<String_value>,

"priority":<Integer_value>,

"secondary":<Boolean_value>,

"groupextraction":<Boolean_value>,

"nextfactor":<String_value>,

"gotopriorityexpression":<String_value>,

"bindpoint":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_responderpolicy_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/authenticationvserver_responderpolicy_binding/ name_value<String> ? **args=policy: <String_value> ,secondary: <Boolean_value> ,groupextraction: <Boolean_value> ,bindpoint: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_responderpolicy_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/authenticationvserver_responderpolicy_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of authenticationvserver_responderpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_responderpolicy_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authenticationvserver_responderpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationvserver_responderpolicy_binding": [ {

"priority":<Integer_value>,

"bindpoint":<String_value>,

"secondary":<Boolean_value>,
```

```
"name":<String_value>,

"nextfactor":<String_value>,

"groupextraction":<Boolean_value>,

"policy":<String_value>,

"gotopriorityexpression":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationvserver_responderpolicy_binding
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/authenticationvserver_responderpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationvserver_responderpolicy_binding": [ {

"priority":<Integer_value>,

"bindpoint":<String_value>,

"secondary":<Boolean_value>,

"name":<String_value>,

"nextfactor":<String_value>,

"groupextraction":<Boolean_value>,

"policy":<String_value>,

"gotopriorityexpression":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_responderpolicy_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"authenticationvserver_responderpolicy_binding": [ { "__count":
"#no"} ] }
```

authenticationvserver_rewritepolicy_binding

Binding object showing the rewritepolicy that can be bound to authenticationvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
groupextraction	<Boolean>	Read-write	Applicable only while bindind classic authentication policy as advance authentication policy use nFactor.
nextfactor	<String>	Read-write	Applicable only while binding advance authentication policy as classic authentication policy does not support nFactor.
gotopriorityexpression	<String>	Read-write	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
policy	<String>	Read-write	The name of the policy, if any, bound to the authentication vserver.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the authentication virtual server to which to bind the policy. Minimum length = 1
secondary	<Boolean>	Read-write	Applicable only while bindind classic authentication policy as advance authentication policy use nFactor.
priority	<Integer>	Read-write	The priority, if any, of the vpn vserver policy.
bindpoint	<String>	Read-write	Bindpoint to which the policy is bound. Possible values = REQUEST, RESPONSE, ICA_REQUEST, OTHERTCP_REQUEST, AAA_REQUEST, AAA_RESPONSE
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)

- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/authenticationvserver_rewritepolicy_binding
HTTP Method: PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"authenticationvserver_rewritepolicy_binding":{

<b>"name":<String_value>,

</b>"policy":<String_value>,

"priority":<Integer_value>,

"secondary":<Boolean_value>,

"groupextraction":<Boolean_value>,

"nextfactor":<String_value>,

"gotopriorityexpression":<String_value>,

"bindpoint":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationvserver_rewritepolicy_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_rewritepolicy_binding/ name_value<String> ? **args=policy: <String_value> ,secondary: <Boolean_value> ,groupextraction: <Boolean_value> ,bindpoint: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationvserver_rewritepolicy_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_rewritepolicy_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of authenticationvserver_rewritepolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_rewritepolicy_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authenticationvserver_rewritepolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationvserver_rewritepolicy_binding": [ {

"groupextraction":<Boolean_value>,

"nextfactor":<String_value>,

"gotopriorityexpression":<String_value>,
```

```
"policy":<String_value>,

"name":<String_value>,

"secondary":<Boolean_value>,

"priority":<Integer_value>,

"bindpoint":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationvserver_rewritepolicy_binding
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/authenticationvserver_rewritepolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationvserver_rewritepolicy_binding": [ {

"groupextraction":<Boolean_value>,

"nextfactor":<String_value>,

"gotopriorityexpression":<String_value>,

"policy":<String_value>,

"name":<String_value>,

"secondary":<Boolean_value>,

"priority":<Integer_value>,

"bindpoint":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationvserver_rewritepolicy_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"authenticationvserver_rewritepolicy_binding": [ { "__count": "#no"} ] }
```

authenticationvserver_tmsessionpolicy_binding

Binding object showing the tmsessionpolicy that can be bound to authenticationvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the authentication virtual server to which to bind the policy. Minimum length = 1
secondary	<Boolean>	Read-write	Applicable only while bindind classic authentication policy as advance authentication policy use nFactor.
bindpoint	<String>	Read-write	Bind point to which to bind the policy. Applies only to rewrite and cache policies. If you do not set this parameter, the policy is bound to REQ_DEFAULT or RES_DEFAULT, depending on whether the policy rule is a response-time or a request-time expression. Possible values = REQUEST, RESPONSE,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			ICA_REQUEST, OTHERTCP_REQUEST, AAA_REQUEST, AAA_RESPONSE
priority	<Integer>	Read-write	The priority, if any, of the vpn vserver policy.
gotopriorityexpression	<String>	Read-write	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
policy	<String>	Read-write	The name of the policy, if any, bound to the authentication vserver.
groupextraction	<Boolean>	Read-write	Applicable only while bindind classic authentication policy as advance authentication policy use nFactor.
nextfactor	<String>	Read-write	Applicable only while binding advance authentication policy as classic authentication policy does not support nFactor.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/authenticationvserver_tmsessionpolicy_binding
HTTP Method: PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"authenticationvserver_tmsessionpolicy_binding":{

<b>"name":<String_value>,

</b>"policy":<String_value>,

"priority":<Integer_value>,

"secondary":<Boolean_value>,

"groupextraction":<Boolean_value>,

"nextfactor":<String_value>,

"gotopriorityexpression":<String_value>,

"bindpoint":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_tmsessionpolicy_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/authenticationvserver_tmsessionpolicy_binding/ name_value<String> ? **args=policy: <String_value> ,secondary: <Boolean_value> ,groupextraction: <Boolean_value> ,bindpoint: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_tmsessionpolicy_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/authenticationvserver_tmsessionpolicy_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of authenticationvserver_tmsessionpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_tmsessionpolicy_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authenticationvserver_tmsessionpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationvserver_tmsessionpolicy_binding": [ {

"name":<String_value>,

"secondary":<Boolean_value>,

"bindpoint":<String_value>,

"priority":<Integer_value>,

"gotopriorityexpression":<String_value>,

"policy":<String_value>,

"groupextraction":<Boolean_value>,

"nextfactor":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationvserver_tmsessionpolicy_binding
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/authenticationvserver_tmsessionpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationvserver_tmsessionpolicy_binding": [ {

"name":<String_value>,

"secondary":<Boolean_value>,

"bindpoint":<String_value>,

"priority":<Integer_value>,

"gotopriorityexpression":<String_value>,

"policy":<String_value>,

"groupextraction":<Boolean_value>,

"nextfactor":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_tmsessionpolicy_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"authenticationvserver_tmsessionpolicy_binding": [ { "__count":
"#no"} ] }
```

authenticationvserver_vpnportaltheme_binding

Binding object showing the vpnportaltheme that can be bound to authenticationvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the authentication virtual server to which to bind the policy. Minimum length = 1
portaltheme	<String>	Read-write	Theme for Authentication virtual server Login portal.
acttype	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)

- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/authenticationvserver_vpnportaltheme_binding
HTTP Method: PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"authenticationvserver_vpnportaltheme_binding":{

<b>"name":<String_value>,

</b>"portaltheme":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationvserver_vpnportaltheme_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_vpnportaltheme_binding/ name_value<String> ? **args=portaltheme: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationvserver_vpnportaltheme_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_vpnportaltheme_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of authenticationvserver_vpnportaltheme_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_vpnportaltheme_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authenticationvserver_vpnportaltheme_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationvserver_vpnportaltheme_binding": [ {

"name":<String_value>,

"portaltheme":<String_value>,

"acttype":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationvserver_vpnportaltheme_binding
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ authenticationvserver_vpnportaltheme_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationvserver_vpnportaltheme_binding": [ {

"name":<String_value>,

"portaltheme":<String_value>,

"acttype":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationvserver_vpnportaltheme_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"authenticationvserver_vpnportaltheme_binding": [ { "__count": "#no"} ] }
```

authenticationwebauthaction

Configuration for Web authentication action resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the Web Authentication action. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after the profile is created.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my authentication action" or 'my authentication action'). Minimum length = 1
serverip	<String>	Read-write	IP address of the web server to be used for authentication. Minimum length = 1
serverport	<Integer>	Read-write	Port on which the web server accepts connections. Minimum value = 1 Range 1 - 65535 * in CLI is represented as 65535 in NITRO API
fullreqexpr	<String>	Read-write	Exact HTTP request, in the form of an expression, which the Citrix ADC sends

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			to the authentication server. The Citrix ADC does not check the validity of this request. One must manually validate the request.
scheme	<String>	Read-write	Type of scheme for the web server. Possible values = http, https
successrule	<String>	Read-write	Expression, that checks to see if authentication is successful.
defaultauthenticationgroup	<String>	Read-write	This is the default group that is chosen when the authentication succeeds in addition to extracted groups.
attribute1	<String>	Read-write	Expression that would be evaluated to extract attribute1 from the webauth response. Maximum length = 128
attribute2	<String>	Read-write	Expression that would be evaluated to extract attribute2 from the webauth response.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum length = 128
attribute3	<String>	Read-write	Expression that would be evaluated to extract attribute3 from the webauth response. Maximum length = 128
attribute4	<String>	Read-write	Expression that would be evaluated to extract attribute4 from the webauth response. Maximum length = 128
attribute5	<String>	Read-write	Expression that would be evaluated to extract attribute5 from the webauth response. Maximum length = 128
attribute6	<String>	Read-write	Expression that would be evaluated to extract attribute6 from the webauth response. Maximum length = 128
attribute7	<String>	Read-write	Expression that would be evaluated to extract attribute7 from the webauth response.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum length = 128
attribute8	<String>	Read-write	Expression that would be evaluated to extract attribute8 from the webauth response. Maximum length = 128
attribute9	<String>	Read-write	Expression that would be evaluated to extract attribute9 from the webauth response. Maximum length = 128
attribute10	<String>	Read-write	Expression that would be evaluated to extract attribute10 from the webauth response. Maximum length = 128
attribute11	<String>	Read-write	Expression that would be evaluated to extract attribute11 from the webauth response. Maximum length = 128
attribute12	<String>	Read-write	Expression that would be evaluated to extract attribute12 from the webauth response.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum length = 128
attribute13	<String>	Read-write	Expression that would be evaluated to extract attribute13 from the webauth response. Maximum length = 128
attribute14	<String>	Read-write	Expression that would be evaluated to extract attribute14 from the webauth response. Maximum length = 128
attribute15	<String>	Read-write	Expression that would be evaluated to extract attribute15 from the webauth response. Maximum length = 128
attribute16	<String>	Read-write	Expression that would be evaluated to extract attribute16 from the webauth response. Maximum length = 128
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationwebauthaction **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationwebauthaction":{

<b>"name":<String_value>,

</b><b>"serverip":<String_value>,

</b><b>"serverport":<Integer_value>,

</b>"fullreqexpr":<String_value>,

<b>"scheme":<String_value>,

</b><b>"successrule":<String_value>,

</b>"defaultauthenticationgroup":<String_value>,

"attribute1":<String_value>,

"attribute2":<String_value>,

"attribute3":<String_value>,

"attribute4":<String_value>,

"attribute5":<String_value>,

"attribute6":<String_value>,

"attribute7":<String_value>,

"attribute8":<String_value>,
```

```
"attribute9":<String_value>,

"attribute10":<String_value>,

"attribute11":<String_value>,

"attribute12":<String_value>,

"attribute13":<String_value>,

"attribute14":<String_value>,

"attribute15":<String_value>,

"attribute16":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationwebauthaction/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationwebauthaction **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationwebauthaction":{

<b>"name":<String_value>,

</b>"serverip":<String_value>,

"serverport":<Integer_value>,

"fullreqexpr":<String_value>,

"scheme":<String_value>,

"successrule":<String_value>,

"defaultauthenticationgroup":<String_value>,

"attribute1":<String_value>,

"attribute2":<String_value>,

"attribute3":<String_value>,

"attribute4":<String_value>,

"attribute5":<String_value>,

"attribute6":<String_value>,

"attribute7":<String_value>,

"attribute8":<String_value>,

"attribute9":<String_value>,

"attribute10":<String_value>,

"attribute11":<String_value>,
```

```
"attribute12":<String_value>,

"attribute13":<String_value>,

"attribute14":<String_value>,

"attribute15":<String_value>,

"attribute16":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationwebauthaction? **action=unset**
HTTP Method: POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationwebauthaction":{

<b>"name":<String_value>,

</b>"serverip":true,

"serverport":true,

"fullreqexpr":true,

"defaultauthenticationgroup":true,
```

```
"attribute1":true,

"attribute2":true,

"attribute3":true,

"attribute4":true,

"attribute5":true,

"attribute6":true,

"attribute7":true,

"attribute8":true,

"attribute9":true,

"attribute10":true,

"attribute11":true,

"attribute12":true,

"attribute13":true,

"attribute14":true,

"attribute15":true,

"attribute16":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationwebauthaction **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/authenticationwebauthaction? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/authenticationwebauthaction? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of authenticationwebauthaction resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/authenticationwebauthaction? **view=summary**

Use this query-parameter to get the summary output of authenticationwebauthaction resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/authenticationwebauthaction? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authenticationwebauthaction resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationwebauthaction": [ {

"name":<String_value>,

"serverip":<String_value>,

"serverport":<Integer_value>,

"fullreqexpr":<String_value>,

"scheme":<String_value>,

"successrule":<String_value>,

"defaultauthenticationgroup":<String_value>,

"attribute1":<String_value>,

"attribute2":<String_value>,

"attribute3":<String_value>,

"attribute4":<String_value>,

"attribute5":<String_value>,

"attribute6":<String_value>,

"attribute7":<String_value>,

"attribute8":<String_value>,

"attribute9":<String_value>,

"attribute10":<String_value>,

"attribute11":<String_value>,

"attribute12":<String_value>,

"attribute13":<String_value>,

"attribute14":<String_value>,
```

```
"attribute15":<String_value>,

"attribute16":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationwebauthaction/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/ authenticationwebauthaction/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/authenticationwebauthaction/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of authenticationwebauthaction resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationwebauthaction": [ {

"name":<String_value>,

"serverip":<String_value>,

"serverport":<Integer_value>,

"fullreqexpr":<String_value>,

"scheme":<String_value>,

"successrule":<String_value>,

"defaultauthenticationgroup":<String_value>,

"attribute1":<String_value>,

"attribute2":<String_value>,

"attribute3":<String_value>,

"attribute4":<String_value>,

"attribute5":<String_value>,

"attribute6":<String_value>,

"attribute7":<String_value>,

"attribute8":<String_value>,

"attribute9":<String_value>,

"attribute10":<String_value>,

"attribute11":<String_value>,

"attribute12":<String_value>,

"attribute13":<String_value>,

"attribute14":<String_value>,
```

```
"attribute15":<String_value>,

"attribute16":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationwebauthaction? **count=yes**
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationwebauthaction": [ { "__count": "#no"} ] }
```

authenticationwebauthpolicy

Configuration for Web authentication policy resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the WebAuth policy. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after LDAP policy is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my authentication policy" or 'my authentication policy'). Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
rule	<String>	Read-write	Name of the Citrix ADC named rule, or an expression, that the policy uses to determine whether to attempt to authenticate the user with the Web server. Minimum length = 1
action	<String>	Read-write	Name of the WebAuth action to perform if the policy matches. Minimum length = 1
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationwebauthpolicy **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationwebauthpolicy":{

<b>"name":<String_value>,

</b><b>"rule":<String_value>,

</b><b>"action":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationwebauthpolicy/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationwebauthpolicy **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authenticationwebauthpolicy":{

<b>"name":<String_value>,

</b>"rule":<String_value>,

"action":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationwebauthpolicy **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/authenticationwebauthpolicy? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/authenticationwebauthpolicy? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of authenticationwebauthpolicy resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/authenticationwebauthpolicy? **view=summary**

Use this query-parameter to get the summary output of authenticationwebauthpolicy resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/authenticationwebauthpolicy? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authenticationwebauthpolicy resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationwebauthpolicy": [ {

"name":<String_value>,

"rule":<String_value>,

"action":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationwebauthpolicy/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/ authenticationwebauthpolicy/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/authenticationwebauthpolicy/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of authenticationwebauthpolicy resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationwebauthpolicy": [ {

"name":<String_value>,

"rule":<String_value>,

"action":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationwebauthpolicy? **count=yes**
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationwebauthpolicy": [ { "__count": "#no"} ] }
```

authenticationwebauthpolicy_authenticationvserver_binding

Binding object showing the authenticationvserver that can be bound to authenticationwebauthpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
boundto	<String>	Read-write	The entity name to which policy is bound.
name	<String>	Read-write	Name of the WebAuth policy. Minimum length = 1
priority	<Integer>	Read-only	.
activepolicy	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationwebauthpolicy_authenticationvserver_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ authenticationwebauthpolicy_authenticationvserver_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of authenticationwebauthpolicy_authenticationvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ authenticationwebauthpolicy_authenticationvserver_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authenticationwebauthpolicy_authenticationvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationwebauthpolicy_authenticationvserver_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"priority":<Integer_value>,

"activepolicy":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationwebauthpolicy_authenticationvserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ authenticationwebauthpolicy_authenticationvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationwebauthpolicy_authenticationvserver_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"priority":<Integer_value>,

"activepolicy":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationwebauthpolicy_authenticationvserver_binding/ name_value<String> ? **count=yes**
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"authenticationwebauthpolicy_authenticationvserver_binding":
[ { "__count": "#no"} ] }
```

authenticationwebauthpolicy_binding

Binding object which returns the resources bound to authenticationwebauthpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the WebAuth policy. Minimum length = 1
authenticationwebauthpolicy_authenticationvserver_binding	<authenticationwebauthpolicy_authenticationvserver_binding[]>	Read-only	authenticationvserver that can be bound to authenticationwebauthpolicy.
authenticationwebauthpolicy_systemglobal_binding	<authenticationwebauthpolicy_systemglobal_binding[]>	Read-only	systemglobal that can be bound to authenticationwebauthpolicy.
authenticationwebauthpolicy_vpnglobal_binding	<authenticationwebauthpolicy_vpnglobal_binding[]>	Read-only	vpnglobal that can be bound to authenticationwebauthpolicy.
authenticationwebauthpolicy_vpnvserver_binding	<authenticationwebauthpolicy_vpnvserver_binding[]>	Read-only	vpnvserver that can be bound to authenticationwebauthpolicy.

Operations

(click to see Properties)

- GET

- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationwebauthpolicy_binding/name_value<String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationwebauthpolicy_binding": [ {

"name":<String_value>,

"authenticationwebauthpolicy_systemglobal_binding":<authenticationwebauthpolicy_systemglobal_binding[]_value>,

"authenticationwebauthpolicy_vpnvserver_binding":<authenticationwebauthpolicy_vpnvserver_binding[]_value>,

"authenticationwebauthpolicy_authenticationvserver_binding":<authenticationwebauthpolicy_authenticationvserver_binding[]_value>,

"authenticationwebauthpolicy_vpnglobal_binding":<authenticationwebauthpolicy_vpnglobal_binding[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/authenticationwebauthpolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/authenticationwebauthpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authenticationwebauthpolicy_binding": [ {

"name":<String_value>,

"authenticationwebauthpolicy_systemglobal_binding":<authenticationwebauthpolicy_systemglobal_binding[]_value>,

"authenticationwebauthpolicy_vpnvserver_binding":<authenticationwebauthpolicy_vpnvserver_binding[]_value>,

"authenticationwebauthpolicy_authenticationvserver_binding":<authenticationwebauthpolicy_authenticationvserver_binding[]_value>,

"authenticationwebauthpolicy_vpnglobal_binding":<authenticationwebauthpolicy_vpnglobal_binding[]_value>

}]}
```

authenticationwebauthpolicy_systemglobal_binding

Binding object showing the systemglobal that can be bound to authenticationwebauthpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the WebAuth policy. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
boundto	<String>	Read-write	The entity name to which policy is bound.
priority	<Integer>	Read-only	.
activepolicy	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationwebauthpolicy_systemglobal_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ authenticationwebauthpolicy_systemglobal_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of authenticationwebauthpolicy_systemglobal_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ authenticationwebauthpolicy_systemglobal_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authenticationwebauthpolicy_systemglobal_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationwebauthpolicy_systemglobal_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"priority":<Integer_value>,

"activepolicy":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationwebauthpolicy_systemglobal_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ authenticationwebauthpolicy_systemglobal_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationwebauthpolicy_systemglobal_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"priority":<Integer_value>,

"activepolicy":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationwebauthpolicy_systemglobal_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"authenticationwebauthpolicy_systemglobal_binding": [ { "__count":
"#no"} ] }
```

authenticationwebauthpolicy_vpnglobal_binding

Binding object showing the vpnglobal that can be bound to authenticationwebauthpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the WebAuth policy. Minimum length = 1
boundto	<String>	Read-write	The entity name to which policy is bound.
priority	<Integer>	Read-only	.
activepolicy	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationwebauthpolicy_vpnglobal_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/authenticationwebauthpolicy_vpnglobal_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of authenticationwebauthpolicy_vpnglobal_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ authenticationwebauthpolicy_vpnglobal_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authenticationwebauthpolicy_vpnglobal_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationwebauthpolicy_vpnglobal_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"priority":<Integer_value>,

"activepolicy":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationwebauthpolicy_vpnglobal_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ authenticationwebauthpolicy_vpnglobal_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationwebauthpolicy_vpnglobal_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"priority":<Integer_value>,

"activepolicy":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationwebauthpolicy_vpnglobal_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"authenticationwebauthpolicy_vpnglobal_binding": [ { "__count":
"#no"} ] }
```

authenticationwebauthpolicy_vpnvserver_binding

Binding object showing the vpnvserver that can be bound to authenticationwebauthpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
boundto	<String>	Read-write	The entity name to which policy is bound.
name	<String>	Read-write	Name of the WebAuth policy. Minimum length = 1
activepolicy	<Integer>	Read-only	.
priority	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationwebauthpolicy_vpnvserver_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/authenticationwebauthpolicy_vpnvserver_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of authenticationwebauthpolicy_vpnvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ authenticationwebauthpolicy_vpnvserver_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authenticationwebauthpolicy_vpnvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationwebauthpolicy_vpnvserver_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"activepolicy":<Integer_value>,

"priority":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationwebauthpolicy_vpnvserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ authenticationwebauthpolicy_vpnvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationwebauthpolicy_vpnvserver_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"activepolicy":<Integer_value>,

"priority":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authenticationwebauthpolicy_vpnvserver_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"authenticationwebauthpolicy_vpnvserver_binding": [ { "__count":
"#no"} ] }
```

authorization

Authorization

Authorization configuration. Authorization services check which resources users are authorized to access, and grant permissions accordingly.

NAME	DESCRIPTION
authorizationaction	Configuration for authorization action
authorizationpolicy	Configuration for authorization policy
authorizationpolicy_aaagroup_binding	Binding object showing the aaagroup that can be bound to authorizationpolicy
authorizationpolicy_aaauser_binding	Binding object showing the aaauser that can be bound to authorizationpolicy
authorizationpolicy_authorizationpolicylabel_binding	Binding object showing the authorizationpolicylabel that can be bound to authorizationpolicy
authorizationpolicy_binding	Binding object showing the resources that can be bound to authorizationpolicy
authorizationpolicy_csvserver_binding	Binding object showing the csvserver that can be bound to authorizationpolicy
authorizationpolicy_lbvserver_binding	Binding object showing the lbvserver that can be bound to authorizationpolicy
authorizationpolicylabel	Configuration for authorization policy label

NAME	DESCRIPTION
authorizationpolicylabel_authorizationpolicy_binding	Binding object showing the authorizationpolicy that can be bound to authorizationpolicylabel
authorizationpolicylabel_binding	Binding object showing the resources that can be bound to authorizationpolicylabel

authorizationaction

Configuration for authorization action resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of authorization action. Minimum length = 1
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/authorizationaction **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/authorizationaction? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/authorizationaction? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of authorizationaction resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/authorizationaction? **view=summary**

Use this query-parameter to get the summary output of authorizationaction resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/authorizationaction? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authorizationaction resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authorizationaction": [ {

"name":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authorizationaction/ name_value<String>
Query-parameters: attrs http:// <netscaler-ip-address> /nitro/v1/config/authorizationaction/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/authorizationaction/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of authorizationaction resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authorizationaction": [ {

"name":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/authorizationaction? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authorizationaction": [ { "__count": "#no"} ] }
```

authorizationpolicy

Configuration for authorization policy resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the new authorization policy. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after the authorization policy is added. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			name in double or single quotation marks (for example, "my authorization policy" or 'my authorization policy'). Minimum length = 1
rule	<String>	Read-write	Name of the Citrix ADC named rule, or an expression, that the policy uses to perform the authentication.
action	<String>	Read-write	Action to perform if the policy matches: either allow or deny the request. Minimum length = 1
newname	<String>	Read-write	The new name of the author policy. Minimum length = 1
activepolicy	<Integer>	Read-only	Indicates whether policy is bound or not.
expressiontype	<String>	Read-only	Type of policy (Classic/Advanced) . Possible values = Classic Policy, Advanced Policy
hits	<Integer>	Read-only	Number of hits.
_nextgenapiresource	<String>	Read-only	.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- RENAME
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/authorizationpolicy **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authorizationpolicy":{

<b>"name":<String_value>,

</b><b>"rule":<String_value>,

</b><b>"action":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/authorizationpolicy/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/authorizationpolicy **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authorizationpolicy":{

<b>"name":<String_value>,

</b>"rule":<String_value>,

"action":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

RENAME

URL: http:// <netscaler-ip-address> /nitro/v1/config/authorizationpolicy? **action=rename HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authorizationpolicy":{

<b>"name":<String_value>,

</b><b>"newname":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/authorizationpolicy **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/authorizationpolicy? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/authorizationpolicy? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of authorizationpolicy resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/authorizationpolicy? **view=summary**

Use this query-parameter to get the summary output of authorizationpolicy resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/authorizationpolicy? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authorizationpolicy resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authorizationpolicy": [ {

"name":<String_value>,

"rule":<String_value>,

"action":<String_value>,

"activepolicy":<Integer_value>,

"expressiontype":<String_value>,

"hits":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authorizationpolicy/ name_value<String>
Query-parameters: attrs http:// <netscaler-ip-address> /nitro/v1/config/authorizationpolicy/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/authorizationpolicy/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of authorizationpolicy resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authorizationpolicy": [ {

"name":<String_value>,

"rule":<String_value>,

"action":<String_value>,

"activepolicy":<Integer_value>,

"expressiontype":<String_value>,

"hits":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/authorizationpolicy? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authorizationpolicy": [ { "__count": "#no"} ] }
```

authorizationpolicy_aaagroup_binding

Binding object showing the aaagroup that can be bound to authorizationpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the authorization policy. Minimum length = 1
boundto	<String>	Read-write	The entity name to which policy is bound.
priority	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authorizationpolicy_aaagroup_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ authorizationpolicy_aaagroup_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of authorizationpolicy_aaagroup_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/authorizationpolicy_aaagroup_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authorizationpolicy_aaagroup_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authorizationpolicy_aaagroup_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"priority":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/authorizationpolicy_aaagroup_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/authorizationpolicy_aaagroup_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authorizationpolicy_aaagroup_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"priority":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/authorizationpolicy_aaagroup_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"authorizationpolicy_aaagroup_binding": [ { "__count": "#no"} ] }
```

authorizationpolicy_aaauser_binding

Binding object showing the aaauser that can be bound to authorizationpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
boundto	<String>	Read-write	The entity name to which policy is bound.
name	<String>	Read-write	Name of the authorization policy. Minimum length = 1
priority	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authorizationpolicy_aaauser_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ authorizationpolicy_aaauser_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of authorizationpolicy_aaauser_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/authorizationpolicy_aaauser_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authorizationpolicy_aaauser_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authorizationpolicy_aaauser_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"priority":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/authorizationpolicy_aaauser_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/authorizationpolicy_aaauser_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authorizationpolicy_aaauser_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"priority":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/authorizationpolicy_aaauser_binding/name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"authorizationpolicy_aaauser_binding": [ { "__count": "#no"} ] }
```

authorizationpolicy_authorizationpolicylabel_binding

Binding object showing the authorizationpolicylabel that can be bound to authorizationpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the authorization policy. Minimum length = 1
boundto	<String>	Read-write	The entity name to which policy is bound.
priority	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authorizationpolicy_authorizationpolicylabel_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ authorizationpolicy_authorizationpolicylabel_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of authorizationpolicy_authorizationpolicylabel_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ authorizationpolicy_authorizationpolicylabel_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authorizationpolicy_authorizationpolicylabel_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authorizationpolicy_authorizationpolicylabel_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"priority":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authorizationpolicy_authorizationpolicylabel_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ authorizationpolicy_authorizationpolicylabel_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authorizationpolicy_authorizationpolicylabel_binding": [ {

"name":<String_value>,
```

```
"boundto":<String_value>,

"priority":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authorizationpolicy_authorizationpolicylabel_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"authorizationpolicy_authorizationpolicylabel_binding": [ { "__count":
"#no"} ] }
```

authorizationpolicy_binding

Binding object which returns the resources bound to authorizationpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the authorization policy. Minimum length = 1
authorizationpolicy_csvserver_binding	<authorizationpolicy_csvserver_binding[]>	Read-only	csvserver that can be bound to authorizationpolicy.
authorizationpolicy_authorizationpolicylabel_binding	<authorizationpolicy_authorizationpolicylabel_binding[]>	Read-only	authorizationpolicylabel that can be bound to authorizationpolicy.
authorizationpolicy_aaagroup_binding	<authorizationpolicy_aaagroup_binding[]>	Read-only	aaagroup that can be bound to authorizationpolicy.
authorizationpolicy_lbvserver_binding	<authorizationpolicy_lbvserver_binding[]>	Read-only	lbvserver that can be bound to authorizationpolicy.
authorizationpolicy_aaauser_binding	<authorizationpolicy_aaauser_binding[]>	Read-only	aaauser that can be bound to authorizationpolicy.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authorizationpolicy_binding/ name_value<String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authorizationpolicy_binding": [ {

"name":<String_value>,
```

```
"authorizationpolicy_authorizationpolicylabel_binding":<authorizationpolic
y_authorizationpolicylabel_binding[]_value>,

"authorizationpolicy_lbvserver_binding":<authorizationpolicy_lbvserver_bin
ding[]_value>,

"authorizationpolicy_csvserver_binding":<authorizationpolicy_csvserver_bin
ding[]_value>,

"authorizationpolicy_aaauser_binding":<authorizationpolicy_aaauser_binding
[]_value>,

"authorizationpolicy_aaagroup_binding":<authorizationpolicy_aaagroup_bindi
ng[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/authorizationpolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/authorizationpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authorizationpolicy_binding": [ {

"name":<String_value>,

"authorizationpolicy_authorizationpolicylabel_binding":<authorizationpolic
y_authorizationpolicylabel_binding[]_value>,

"authorizationpolicy_lbvserver_binding":<authorizationpolicy_lbvserver_bin
ding[]_value>,

"authorizationpolicy_csvserver_binding":<authorizationpolicy_csvserver_bin
ding[]_value>,

"authorizationpolicy_aaauser_binding":<authorizationpolicy_aaauser_binding
[]_value>,

"authorizationpolicy_aaagroup_binding":<authorizationpolicy_aaagroup_bindi
ng[]_value>

}]}
```

authorizationpolicy_csvserver_binding

Binding object showing the csvserver that can be bound to authorizationpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
boundto	<String>	Read-write	The entity name to which policy is bound.
name	<String>	Read-write	Name of the authorization policy. Minimum length = 1
priority	<Integer>	Read-only	.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authorizationpolicy_csvserver_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ authorizationpolicy_csvserver_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of authorizationpolicy_csvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/authorizationpolicy_csvserver_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authorizationpolicy_csvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authorizationpolicy_csvserver_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"priority":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/authorizationpolicy_csvserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/authorizationpolicy_csvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authorizationpolicy_csvserver_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"priority":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/authorizationpolicy_csvserver_binding/name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"authorizationpolicy_csvserver_binding": [ { "__count": "#no"} ] }
```

authorizationpolicy_lbvserver_binding

Binding object showing the lbvserver that can be bound to authorizationpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
boundto	<String>	Read-write	The entity name to which policy is bound.
name	<String>	Read-write	Name of the authorization policy. Minimum length = 1
priority	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET

- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authorizationpolicy_lbvserver_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ authorizationpolicy_lbvserver_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of authorizationpolicy_lbvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/authorizationpolicy_lbvserver_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authorizationpolicy_lbvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authorizationpolicy_lbvserver_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"priority":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/authorizationpolicy_lbvserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/authorizationpolicy_lbvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authorizationpolicy_lbvserver_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"priority":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/authorizationpolicy_lbvserver_binding/name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"authorizationpolicy_lbvserver_binding": [ { "__count": "#no"} ] }
```

authorizationpolicylabel

Configuration for authorization policy label resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
labelname	<String>	Read-write	Name for the new authorization policy label. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after the authorization policy is created. The following requirement applies only to the Citrix ADC CLI:

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my authorization policy label" or 'authorization policy label').
newname	<String>	Read-write	The new name of the auth policy label. Minimum length = 1
numpol	<Integer>	Read-only	Number of polices bound to label.
hits	<Integer>	Read-only	Number of times policy label was invoked.
policyname	<String>	Read-only	Name of the authorization policy to bind to the policy label.
priority	<Integer>	Read-only	Specifies the priority of the policy.
gotopriorityexpression	<String>	Read-only	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
labeltype	<String>	Read-only	Type of invocation. Available settings function as follows: * reqvserver - Send the request to the specified request virtual server. * resvserver - Send the response to the specified response virtual server. * policylabel - Invoke the specified policy label. Possible values = reqvserver, resvserver, policylabel
invoke_labelname	<String>	Read-only	Name of the policy label to invoke if the current policy evaluates to TRUE, the invoke parameter is set, and Label Type is set to Policy Label.
flowtype	<Integer>	Read-only	Flowtype of the bound authorization policy.
description	<String>	Read-only	Description of the policylabel.
_nextgenapiresource	<String>	Read-only	.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- RENAME
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/authorizationpolicylabel **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authorizationpolicylabel":{

<b>"labelname":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/authorizationpolicylabel/ labelname_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

RENAME

URL: http:// <netscaler-ip-address> /nitro/v1/config/authorizationpolicylabel? **action=rename** **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"authorizationpolicylabel":{

<b>"labelname":<String_value>,

</b><b>"newname":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/authorizationpolicylabel **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/authorizationpolicylabel? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/authorizationpolicylabel? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of authorizationpolicylabel resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/authorizationpolicylabel? **view=summary**

Use this query-parameter to get the summary output of authorizationpolicylabel resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/authorizationpolicylabel? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authorizationpolicylabel resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authorizationpolicylabel": [ {

"labelname":<String_value>,

"numpol":<Integer_value>,

"hits":<Integer_value>,

"policyname":<String_value>,

"priority":<Integer_value>,

"gotopriorityexpression":<String_value>,

"labeltype":<String_value>,

"invoke_labelname":<String_value>,

"flowtype":<Integer_value>,

"description":<String_value>,

"_nextgenapiresource":<String_value>
```

```
}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authorizationpolicylabel/ labelname_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/ authorizationpolicylabel/ labelname_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/authorizationpolicylabel/ labelname_value<String> ? **view=summary**

Use this query-parameter to get the summary output of authorizationpolicylabel resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authorizationpolicylabel": [ {

"labelname":<String_value>,

"numpol":<Integer_value>,
```

```
"hits":<Integer_value>,

"policyname":<String_value>,

"priority":<Integer_value>,

"gotopriorityexpression":<String_value>,

"labeltype":<String_value>,

"invoke_labelname":<String_value>,

"flowtype":<Integer_value>,

"description":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/authorizationpolicylabel? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authorizationpolicylabel": [ { "__count": "#no"} ] }
```

authorizationpolicylabel_authorizationpolicy_binding

Binding object showing the authorizationpolicy that can be bound to authorizationpolicylabel.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
labeltype	<String>	Read-write	Type of invocation. Available settings function as follows: * reqvserver - Send the request to the specified request virtual server. * resvserver - Send the response to the specified response virtual server. * policylabel - Invoke the specified policy label. Possible values = reqvserver, resvserver, policylabel
priority	<Integer>	Read-write	Specifies the priority of the policy.
labelname	<String>	Read-write	Name of the authorization policy label to which to bind the policy.
policyname	<String>	Read-write	Name of the authorization policy

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			to bind to the policy label.
gotopriorityexpression	<String>	Read-write	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
invoke	<Boolean>	Read-write	If the current policy evaluates to TRUE, terminate evaluation of policies bound to the current policy label, and then either forward the request or response to the specified virtual server or evaluate the specified policy label.
invoke_labelname	<String>	Read-write	Name of the policy label to invoke if the current policy evaluates to TRUE, the invoke parameter is set, and Label Type is set to Policy Label.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/authorizationpolicylabel_authorizationpolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"authorizationpolicylabel_authorizationpolicy_binding":{

<b>"labelname":<String_value>,

</b><b>"policyname":<String_value>,

</b><b>"priority":<Integer_value>,

</b>"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>,

"labeltype":<String_value>,

"invoke_labelname":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authorizationpolicylabel_authorizationpolicy_binding/ labelname_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ authorizationpolicylabel_authorizationpolicy_binding/ labelname_value<String> ? **args= policyname:<String_value>, priority: <Integer_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authorizationpolicylabel_authorizationpolicy_binding/ labelname_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ authorizationpolicylabel_authorizationpolicy_binding/ labelname_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of authorizationpolicylabel_authorizationpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ authorizationpolicylabel_authorizationpolicy_binding/ labelname_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the authorizationpolicylabel_authorizationpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authorizationpolicylabel_authorizationpolicy_binding": [ {

"labeltype":<String_value>,

"priority":<Integer_value>,
```

```
"labelname":<String_value>,

"policyname":<String_value>,

"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>,

"invoke_labelname":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authorizationpolicylabel_authorizationpolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ authorizationpolicylabel_authorizationpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authorizationpolicylabel_authorizationpolicy_binding": [ {

"labeltype":<String_value>,

"priority":<Integer_value>,

"labelname":<String_value>,

"policyname":<String_value>,

"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>,

"invoke_labelname":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/ authorizationpolicylabel_authorizationpolicy_binding/ labelname_value<String> ? **count=yes**
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"authorizationpolicylabel_authorizationpolicy_binding": [ { "__count":
"#no"} ] }
```

authorizationpolicylabel_binding

Binding object which returns the resources bound to authorizationpolicylabel.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
labelname	<String>	Read-write	Name of the authorization policy label.
authorizationpolicylabel_authorizationpolicy_binding	<authorizationpolicylabel_authorizationpolicy_binding[]>	Read-only	authorizationpolicy that can be bound to authorizationpolicylabel.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.
- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of

creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/authorizationpolicylabel_binding/ labelname_value<String>

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authorizationpolicylabel_binding": [ {

"labelname":<String_value>,
```

```
"authorizationpolicylabel_authorizationpolicy_binding":<authorizationpolic
ylabel_authorizationpolicy_binding[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/authorizationpolicylabel_binding

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters:

bulkbindings

http:// <netscaler-ip-address> /nitro/v1/config/authorizationpolicylabel_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "authorizationpolicylabel_binding": [ {

"labelname":<String_value>,

"authorizationpolicylabel_authorizationpolicy_binding":<authorizationpolic
ylabel_authorizationpolicy_binding[]_value>

}]}
```

autoscale

Autoscale

AutoScale configuration.

NAME	DESCRIPTION
autoscaleaction	Configuration for autoscale action
autoscalepolicy	Configuration for Autoscale policy
autoscalepolicy_binding	Binding object showing the resources that can be bound to autoscalepolicy
autoscalepolicy_nstimer_binding	Binding object showing the nstimer that can be bound to autoscalepolicy
autoscaleprofile	Configuration for autoscale profile

autoscaleaction

Configuration for autoscale action resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	ActionScale action name. Minimum length = 1
type	<String>	Read-write	The type of action. Possible values = SCALE_UP, SCALE_DOWN
profilename	<String>	Read-write	AutoScale profile name. Minimum length = 1
parameters	<String>	Read-write	Parameters to use in the action. Minimum length = 1
vmdestroygraceperiod	<Integer>	Read-write	Time in minutes a VM is kept in inactive state before destroying. Default value: 10
quiettime	<Integer>	Read-write	Time in seconds no other policy is evaluated or action is taken. Default value: 300
vserver	<String>	Read-write	Name of the vserver on which autoscale action has to be taken.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/autoscaleaction/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/autoscaleaction **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"autoscaleaction":{

<b>"name":<String_value>,

</b>"profilename":<String_value>,

"parameters":<String_value>,

"vmdestroygraceperiod":<Integer_value>,

"quiettime":<Integer_value>,

"vserver":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/autoscaleaction? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"autoscaleaction":{

<b>"name":<String_value>,

</b>"vmdestroygraceperiod":true,

"quiettime":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/autoscaleaction **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"autoscaleaction":{

<b>"name":<String_value>,

</b><b>"type":<String_value>,

</b><b>"profilename":<String_value>,

</b><b>"parameters":<String_value>,
```

```
</b>"vmdestroygraceperiod":<Integer_value>,

"quiettime":<Integer_value>,

<b>"vserver":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/autoscaleaction **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/autoscaleaction? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/autoscaleaction? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of autoscaleaction resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/autoscaleaction? **view=summary**

Use this query-parameter to get the summary output of autoscaleaction resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/autoscaleaction? **pagesize=#no;pageno=#no**

Use this query-parameter to get the autoscaleaction resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "autoscaleaction": [ {

"name":<String_value>,

"type":<String_value>,

"profilename":<String_value>,

"parameters":<String_value>,

"vmdestroygraceperiod":<Integer_value>,

"quiettime":<Integer_value>,

"vserver":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/autoscaleaction/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/autoscaleaction/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/autoscaleaction/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of autoscaleaction resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "autoscaleaction": [ {

"name":<String_value>,

"type":<String_value>,

"profilename":<String_value>,

"parameters":<String_value>,

"vmdestroygraceperiod":<Integer_value>,

"quiettime":<Integer_value>,

"vserver":<String_value>,

"_nextgenapiresource":<String_value>
```

```
}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/autoscaleaction? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "autoscaleaction": [ { "__count": "#no"} ] }
```

autoscalepolicy

Configuration for Autoscale policy resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	The name of the autoscale policy. Minimum length = 1
rule	<String>	Read-write	The rule associated with the policy.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
action	<String>	Read-write	The autoscale profile associated with the policy. Minimum length = 1
comment	<String>	Read-write	Comments associated with this autoscale policy.
logaction	<String>	Read-write	The log action associated with the autoscale policy.
newname	<String>	Read-write	The new name of the autoscale policy. Minimum length = 1
hits	<Integer>	Read-only	Number of hits.
undefhits	<Integer>	Read-only	Number of Undef hits.
priority	<Integer>	Read-only	Specifies the priority of the policy.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET

- COUNT
- RENAME

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

RENAME

URL: http:// <netscaler-ip-address> /nitro/v1/config/autoscalepolicy? **action=rename HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"autoscalepolicy":{

<b>"name":<String_value>,

</b><b>"newname":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/autoscalepolicy/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/autoscalepolicy **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"autoscalepolicy":{

<b>"name":<String_value>,

</b>"rule":<String_value>,
```

```
"action":<String_value>,

"comment":<String_value>,

"logaction":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/autoscalepolicy? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"autoscalepolicy":{

<b>"name":<String_value>,

</b>"rule":true,

"action":true,

"comment":true,

"logaction":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/autoscalepolicy **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"autoscalepolicy":{

<b>"name":<String_value>,

</b><b>"rule":<String_value>,

</b><b>"action":<String_value>,

</b>"comment":<String_value>,

"logaction":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/autoscalepolicy **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/autoscalepolicy? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/autoscalepolicy? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of autoscalepolicy resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/autoscalepolicy? **view=summary**

Use this query-parameter to get the summary output of autoscalepolicy resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/autoscalepolicy? **pagesize=#no;pageno=#no**

Use this query-parameter to get the autoscalepolicy resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "autoscalepolicy": [ {

"name":<String_value>,

"rule":<String_value>,

"action":<String_value>,

"comment":<String_value>,

"logaction":<String_value>,
```

```
"hits":<Integer_value>,

"undefhits":<Integer_value>,

"priority":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/autoscalepolicy/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/autoscalepolicy/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/autoscalepolicy/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of autoscalepolicy resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "autoscalepolicy": [ {

"name":<String_value>,

"rule":<String_value>,

"action":<String_value>,

"comment":<String_value>,

"logaction":<String_value>,

"hits":<Integer_value>,

"undefhits":<Integer_value>,

"priority":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/autoscalepolicy? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "autoscalepolicy": [ { "__count": "#no"} ] }
```

autoscalepolicy_binding

Binding object which returns the resources bound to autoscalepolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	The name of the autoscale policy. Minimum length = 1
autoscalepolicy_nstimer_binding	<autoscalepolicy_nstimer_binding[]>	Read-only	nstimer that can be bound to autoscalepolicy.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.
- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of

creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/autoscalepolicy_binding/ name_value<String>
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "autoscalepolicy_binding": [ {

"name":<String_value>,

"autoscalepolicy_nstimer_binding":<autoscalepolicy_nstimer_binding[]_value
>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/autoscalepolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/autoscalepolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "autoscalepolicy_binding": [ {

"name":<String_value>,

"autoscalepolicy_nstimer_binding":<autoscalepolicy_nstimer_binding[]_value
>

}]}
```

autoscalepolicy_nstimer_binding

Binding object showing the nstimer that can be bound to autoscalepolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
boundto	<String>	Read-write	Location where policy is bound.
name	<String>	Read-write	The name of the autoscale policy. Minimum length = 1
priority	<Integer>	Read-only	Specifies the priority of the policy.
gotopriorityexpression	<String>	Read-only	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/autoscalepolicy_nstimer_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ autoscalepolicy_nstimer_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of autoscalepolicy_nstimer_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/autoscalepolicy_nstimer_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the autoscalepolicy_nstimer_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "autoscalepolicy_nstimer_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"priority":<Integer_value>,

"gotopriorityexpression":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/autoscalepolicy_nstimer_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/autoscalepolicy_nstimer_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "autoscalepolicy_nstimer_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"priority":<Integer_value>,

"gotopriorityexpression":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/autoscalepolicy_nstimer_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"autoscalepolicy_nstimer_binding": [ { "__count": "#no"} ] }
```

autoscaleprofile

Configuration for autoscale profile resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	AutoScale profile name. Minimum length = 1
type	<String>	Read-write	The type of profile. Possible values = CLOUDSTACK
url	<String>	Read-write	URL providing the service. Minimum length = 1
apikey	<String>	Read-write	api key for authentication with service. Minimum length = 1
sharedsecret	<String>	Read-write	shared secret for authentication with service. Minimum length = 1
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- GET (ALL)
- GET

- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/autoscaleprofile **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"autoscaleprofile":{

<b>"name":<String_value>,
```

```
</b><b>"type":<String_value>,

</b><b>"url":<String_value>,

</b><b>"apikey":<String_value>,

</b><b>"sharedsecret":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/autoscaleprofile/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/autoscaleprofile **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"autoscaleprofile":{

<b>"name":<String_value>,
```

```
</b>"url":<String_value>,

"apikey":<String_value>,

"sharedsecret":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/autoscaleprofile **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/autoscaleprofile? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/autoscaleprofile? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of autoscaleprofile resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/autoscaleprofile? **view=summary**

Use this query-parameter to get the summary output of autoscaleprofile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/autoscaleprofile? **pagesize=#no;pageno=#no**

Use this query-parameter to get the autoscaleprofile resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "autoscaleprofile": [ {

"name":<String_value>,

"type":<String_value>,

"url":<String_value>,

"apikey":<String_value>,

"sharedsecret":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/autoscaleprofile/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/autoscaleprofile/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/autoscaleprofile/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of autoscaleprofile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "autoscaleprofile": [ {

"name":<String_value>,

"type":<String_value>,

"url":<String_value>,

"apikey":<String_value>,

"sharedsecret":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/autoscaleprofile? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "autoscaleprofile": [ { "__count": "#no"} ] }
```

azure

Azure

Azure configuration

NAME	DESCRIPTION
azureapplication	Configuration for Azure Application
azurekeyvault	Configuration for Azure Key Vault entity

azureapplication

Configuration for Azure Application resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the application. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at sign (@), equal sign (=), and hyphen (-) characters. Can be changed after the application is created.', CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my application" or 'my application'). Minimum length = 1 Maximum length = 31
clientid	<String>	Read-write	Application ID that is generated when an application is created in Azure Active Directory using either the Azure CLI or the Azure portal (GUI).

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum length = 1 Maximum length = 223
clientsecret	<String>	Read-write	Password for the application configured in Azure Active Directory. The password is specified in the Azure CLI or generated in the Azure portal (GUI). Minimum length = 1 Maximum length = 223
tenantid	<String>	Read-write	ID of the directory inside Azure Active Directory in which the application was created. Minimum length = 1 Maximum length = 220
vaultresource	<String>	Read-write	Vault resource for which access token is granted. Example : vault.azure.net. Minimum length = 3 Maximum length = 254
tokenendpoint	<String>	Read-write	URL from where access token can be obtained. If the token

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			end point is not specified, the default value is https://login.microsoftonline.com/<tenant id>. Minimum length = 1 Maximum length = 255
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/azureapplication **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"azureapplication":{

<b>"name":<String_value>,

</b>"clientid":<String_value>,

"clientsecret":<String_value>,

"tenantid":<String_value>,

<b>"vaultresource":<String_value>,

</b>"tokenendpoint":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/azureapplication/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/azureapplication **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/azureapplication? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/azureapplication? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of azureapplication resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/azureapplication? **view=summary**

Use this query-parameter to get the summary output of azureapplication resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/azureapplication? **pagesize=#no;pageno=#no**

Use this query-parameter to get the azureapplication resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "azureapplication": [ {

"name":<String_value>,

"clientid":<String_value>,

"tokenendpoint":<String_value>,

"tenantid":<String_value>,

"vaultresource":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/azureapplication/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/azureapplication/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/azureapplication/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of azureapplication resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "azureapplication": [ {

"name":<String_value>,

"clientid":<String_value>,

"tokenendpoint":<String_value>,

"tenantid":<String_value>,

"vaultresource":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/azureapplication? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "azureapplication": [ { "__count": "#no"} ] }
```

azurekeyvault

Configuration for Azure Key Vault entity resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the Key Vault. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at sign (@), equal sign (=), and hyphen (-) characters. Can be

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			changed after the Key Vault is created. CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my keyvault" or 'my keyvault'). Minimum length = 1
azurevaultname	<String>	Read-write	Name of the Key Vault configured in Azure cloud using either the Azure CLI or the Azure portal (GUI) with complete domain name. Example: Test.vault.azure.net. Minimum length = 3 Maximum length = 255
azureapplication	<String>	Read-write	Name of the Azure Application object created on the ADC appliance. This object will be used for authentication with Azure Active Directory. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum length = 63
state	<String>	Read-only	Current state of keyvault. Possible values = Created, Could not reach token endpoint, Authorization failed, Token parse error, Access token obtained, Keyvault host is reachable, Keyvault operation succeeded, Keyvault operation failed, Ops failed. Keyvault marked down
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/azurekeyvault/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/azurekeyvault **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"azurekeyvault":{

<b>"name":<String_value>,

</b>"azurevaultname":<String_value>,

<b>"azureapplication":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/azurekeyvault **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/azurekeyvault? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/azurekeyvault? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of azurekeyvault resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/azurekeyvault? **view=summary**

Use this query-parameter to get the summary output of azurekeyvault resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/azurekeyvault? **pagesize=#no;pageno=#no**

Use this query-parameter to get the azurekeyvault resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "azurekeyvault": [ {

"name":<String_value>,

"azurevaultname":<String_value>,

"azureapplication":<String_value>,

"state":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/azurekeyvault/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/azurekeyvault/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/azurekeyvault/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of azurekeyvault resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "azurekeyvault": [ {

"name":<String_value>,

"azurevaultname":<String_value>,

"azureapplication":<String_value>,

"state":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/azurekeyvault? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "azurekeyvault": [ { "__count": "#no"} ] }
```

basic

Basic

Basic system configuration.

NAME	DESCRIPTION
dbsmonitors	Configuration for DB monitors
extendedmemoryparam	Configuration for Parameter for extended memory used by LSN and Subscriber Store
location	Configuration for location
locationdata	Configuration for location data
locationfile	Configuration for location file

NAME	DESCRIPTION
locationfile6	Configuration for location file6
locationparameter	Configuration for location parameter
mcpprofile	Configuration for mcpProfile
nstrace	Configuration for nstrace operations
radiusnode	Configuration for RADIUS Node
server	Configuration for server
server_binding	Binding object showing the resources that can be bound to server
server_gslbservice_binding	Binding object showing the gslbservice that can be bound to server
server_gslbservicegroup_binding	Binding object showing the gslbservicegroup that can be bound to server
server_service_binding	Binding object showing the service that can be bound to server
server_servicegroup_binding	Binding object showing the servicegroup that can be bound to server
service	Configuration for service
service_binding	Binding object showing the resources that can be bound to service
service_lbmonitor_binding	Binding object showing the lbmonitor that can be bound to service
servicegroup	Configuration for service group

NAME	DESCRIPTION
servicegroup_binding	Binding object showing the resources that can be bound to servicegroup
servicegroup_lbmonitor_binding	Binding object showing the lbmonitor that can be bound to servicegroup
servicegroup_servicegroupentitymonbindings_binding	Binding object showing the servicegroupentitymonbindings that can be bound to servicegroup
servicegroup_servicegroupmember_binding	Binding object showing the servicegroupmember that can be bound to servicegroup
servicegroup_servicegroupmemberlist_binding	Binding object showing the servicegroupmemberlist that can be bound to servicegroup
servicegroupbindings	Configuration for servicegroupbind
svcbindings	Configuration for service bindings
vserver	Configuration for virtual server

dbsmonitors

Configuration for DB monitors resource.

Operations

- RESTART

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

RESTART

URL: http:// <netscaler-ip-address> /nitro/v1/config/dbsmonitors? **action=restart**

HTTP Method: POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"dbsmonitors":{

}}
```

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

extendedmemoryparam

Configuration for Parameter for extended memory used by LSN and Subscriber Store resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
memlimit	<Integer>	Read-write	Amount of NetScaler memory to reserve for the memory used by LSN and Subscriber Session Store feature, in multiples of 2MB. Note: If you later reduce the value of this parameter, the amount of active memory is not reduced. Changing the configured memory limit can only increase the amount of active memory.
memlimitactive	<Integer>	Read-only	The active memory limit for extendedmemory on the system. Active memory limit could be different from configured memory limit. This could happen when memory limit could

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			not be increased due to unavailability, or could not be decreased as it is already in use. This active memory limit configures the current memory limit for LSN and Subscriber Session Store.
maxmemlimit	<Integer>	Read-only	The maximum value of memory limit for extendedmemory on the system. Actual available memory may be less. This is maximum memory that can be utilized by LSN and Subscriber Session Store modules.
minrequiredmemory	<Integer>	Read-only	The minimum memory requirement for extendedmemory. This is minimum memory required for LSN and Subscriber Session Store Modules.
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- UPDATE
- UNSET

- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/extendedmemoryparam **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"extendedmemoryparam":{

"memlimit":<Integer_value>
```

```
}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/extendedmemoryparam? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"extendedmemoryparam":{

"memlimit":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/extendedmemoryparam **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "extendedmemoryparam": [ {

"memlimitactive":<Integer_value>,

"maxmemlimit":<Integer_value>,

"memlimit":<Integer_value>,

"minrequiredmemory":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

location

Configuration for location resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ipfrom	<String>	Read-write	First IP address in the range, in dotted decimal notation. Minimum length = 1
ipto	<String>	Read-write	Last IP address in the range, in dotted decimal notation. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
preferredlocation	<String>	Read-write	String of qualifiers, in dotted notation, describing the geographical location of the IP address range. Each qualifier is more specific than the one that precedes it, as in continent.country.region.city.isp.organization. For example, "NA.US.CA.San Jose.ATT.citrix". Note: A qualifier that includes a dot (.) or space ( ) must be enclosed in double quotation marks. Minimum length = 1
longitude	<Integer>	Read-write	Numerical value, in degrees, specifying the longitude of the geographical location of the IP address-range. Note: Longitude and latitude parameters are used for selecting a service with the static proximity GSLB method. If they are not specified, selection is based on the qualifiers

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			specified for the location. Minimum value = -180 Maximum value = 180
latitude	<Integer>	Read-write	Numerical value, in degrees, specifying the latitude of the geographical location of the IP address-range. Note: Longitude and latitude parameters are used for selecting a service with the static proximity GSLB method. If they are not specified, selection is based on the qualifiers specified for the location. Minimum value = -90 Maximum value = 90
q1label	<String>	Read-only	Least specific location qualifier.
q2label	<String>	Read-only	Location qualifier 2.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
q3label	<String>	Read-only	Location qualifier 3.
q4label	<String>	Read-only	Location qualifier 4.
q5label	<String>	Read-only	Location qualifier 5.
q6label	<String>	Read-only	Most specific location qualifier.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.
- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/location **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"location":{

<b>"ipfrom":<String_value>,

</b><b>"ipto":<String_value>,

</b><b>"preferredlocation":<String_value>,

</b>"longitude":<Integer_value>,

"latitude":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/location/ ipfrom_value<String> **Query-parameters: args= ipto:<String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/location **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/location? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/location? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of location resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/location? **view=summary**

Use this query-parameter to get the summary output of location resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/location? **pagesize=#no;pageno=#no**

Use this query-parameter to get the location resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "location": [ {

"ipfrom":<String_value>,

"ipto":<String_value>,

"preferredlocation":<String_value>,

"q1label":<String_value>,

"q2label":<String_value>,

"q3label":<String_value>,

"q4label":<String_value>,

"q5label":<String_value>,

"q6label":<String_value>,

"longitude":<Integer_value>,

"latitude":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/location/ ipfrom_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/location/ ipfrom_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/location/ ipfrom_value<String> ? **view=summary**

Use this query-parameter to get the summary output of location resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "location": [ {

"ipfrom":<String_value>,

"ipto":<String_value>,

"preferredlocation":<String_value>,

"q1label":<String_value>,
```

```
"q2label":<String_value>,

"q3label":<String_value>,

"q4label":<String_value>,

"q5label":<String_value>,

"q6label":<String_value>,

"longitude":<Integer_value>,

"latitude":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/location? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "location": [ { "__count": "#no"} ] }
```

locationdata

Configuration for location data resource.

Operations

- CLEAR

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

CLEAR

URL: http:// <netscaler-ip-address> /nitro/v1/config/locationdata? **action=clear**

HTTP Method: POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"locationdata":{

}}
```

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

locationfile

Configuration for location file resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
Locationfile	<String>	Read-write	Name of the location file, with or without absolute path. If the path is not included, the default path (/var/netscaler/locdb) is assumed. In a high availability setup, the static database must be stored in the same location on both NetScalers. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
format	<String>	Read-write	Format of the location file. Required for the NetScaler to identify how to read the location file. Default value: netscaler Possible values = netscaler, ip-country, ip-country-isp, ip-country-region-city, ip-country-region-city-isp, geoip-country, geoip-region, geoip-city, geoip-country-org, geoip-country-isp, geoip-city-isp-org
src	<String>	Read-write	URL \(protocol, host, path, and file name\) from where the location file will be imported. NOTE: The import fails if the object to be imported is on an HTTPS server that requires client certificate authentication for access. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum length = 2047
curlocfilestatus	<String>	Read-only	The status of the current location file. Default value: Active Possible values = Not Loaded, Active, In Progress, Failed
prevlocationfile	<String>	Read-only	The name of the previous location file. Minimum length = 1
prevlocfileformat	<String>	Read-only	The format of the previous location file. Default value: netscaler Possible values = netscaler, ip-country, ip-country-isp, ip-country-region-city, ip-country-region-city-isp, geoip-country, geoip-region, geoip-city, geoip-country-org, geoip-country-isp, geoip-city-isp-org
prevlocfilestatus	<String>	Read-only	The status of the previous location file. Default value: Active

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = Not Loaded, Active, In Progress, Failed
locfilestatusstr	<String>	Read-only	Status string of the location file.
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- ADD
- DELETE
- GET (ALL)
- IMPORT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/locationfile **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"locationfile":{

<b>"Locationfile":<String_value>,

</b>"format":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/locationfile **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

IMPORT

URL: http:// <netscaler-ip-address> /nitro/v1/config/locationfile? **action=Import HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"locationfile":{

<b>"Locationfile":<String_value>,

</b><b>"src":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/locationfile **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "locationfile": [ {

"Locationfile":<String_value>,

"format":<String_value>,

"curlocfilestatus":<String_value>,

"prevlocationfile":<String_value>,

"prevlocfileformat":<String_value>,

"prevlocfilestatus":<String_value>,

"locfilestatusstr":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

locationfile6

Configuration for location file6 resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
Locationfile	<String>	Read-write	Name of the IPv6 location file, with or without absolute path. If the path is not included, the default path (/var/netscaler/locdb) is assumed. In a high availability setup, the static database must be stored in the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			same location on both NetScalers. Minimum length = 1
format	<String>	Read-write	Format of the IPv6 location file. Required for the NetScaler to identify how to read the location file. Default value: netscaler6 Possible values = netscaler6, geoip-country6
src	<String>	Read-write	URL \(protocol, host, path, and file name\) from where the location file will be imported. NOTE: The import fails if the object to be imported is on an HTTPS server that requires client certificate authentication for access. Minimum length = 1 Maximum length = 2047
curlocfilestatus	<String>	Read-only	The status of the current location file.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: Active Possible values = Not Loaded, Active, In Progress, Failed
prevlocationfile	<String>	Read-only	The name of the previous location file. Minimum length = 1
prevlocfileformat	<String>	Read-only	The format of the previous location file. Default value: NSMAP_FORMAT_NETSCALER Possible values = netscaler6, geoip-country6
prevlocfilestatus	<String>	Read-only	The status of the previous location file. Default value: Active Possible values = Not Loaded, Active, In Progress, Failed
locfilestatusstr	<String>	Read-only	Status string of the location file.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET (ALL)
- COUNT
- IMPORT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/locationfile6 **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"locationfile6":{

<b>"Locationfile":<String_value>,

</b>"format":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/locationfile6 **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

IMPORT

URL: http:// <netscaler-ip-address> /nitro/v1/config/locationfile6? **action=Import HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"locationfile6":{

<b>"Locationfile":<String_value>,
```

```
</b><b>"src":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/locationfile6 **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/locationfile6? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/locationfile6? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of locationfile6 resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/locationfile6? **view=summary**

Use this query-parameter to get the summary output of locationfile6 resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/locationfile6? **pagesize=#no;pageno=#no**

Use this query-parameter to get the locationfile6 resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "locationfile6": [ {

"Locationfile":<String_value>,

"format":<String_value>,

"curlocfilestatus":<String_value>,

"prevlocationfile":<String_value>,

"prevlocfileformat":<String_value>,

"prevlocfilestatus":<String_value>,

"locfilestatusstr":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/locationfile6? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "locationfile6": [ { "__count": "#no"} ] }
```

locationparameter

Configuration for location parameter resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
context	<String>	Read-write	Context for describing locations. In geographic context, qualifier labels are assigned by default in the following sequence: Continent.Country.Region.City.ISP.Organization. In custom context, the qualifiers labels can have any meaning that you designate. Possible values = geographic, custom
q1label	<String>	Read-write	Label specifying the meaning of the first qualifier. Can be specified for custom context only. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
q2label	<String>	Read-write	Label specifying the meaning of the second qualifier. Can be specified for custom context only. Minimum length = 1
q3label	<String>	Read-write	Label specifying the meaning of the third qualifier. Can be specified for custom context only. Minimum length = 1
q4label	<String>	Read-write	Label specifying the meaning of the fourth qualifier. Can be specified for custom context only. Minimum length = 1
q5label	<String>	Read-write	Label specifying the meaning of the fifth qualifier. Can be specified for custom context only. Minimum length = 1
q6label	<String>	Read-write	Label specifying the meaning of the sixth qualifier. Can be specified for custom context only. Minimum length = 1
matchwildcardtoany	<String>	Read-write	Indicates whether wildcard qualifiers should match any other

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			qualifier including non-wildcard while evaluating location based expressions. Possible values: Yes, No, Expression. Yes - Wildcard qualifiers match any other qualifiers. No - Wildcard qualifiers do not match non-wildcard qualifiers, but match other wildcard qualifiers. Expression - Wildcard qualifiers in an expression match any qualifier in an LDNS location, wildcard qualifiers in the LDNS location do not match non-wildcard qualifiers in an expression.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: NO Possible values = YES, NO, Expression
Locationfile	<String>	Read-only	Currently loaded location database file.
format	<String>	Read-only	Location file format. Possible values = netscaler, ip-country, ip-country-isp, ip-country-region-city, ip-country-region-city-isp, geoip-country, geoip-region, geoip-city, geoip-country-org, geoip-country-isp, geoip-city-isp-org
custom	<Integer>	Read-only	Number of configured custom locations.
Static	<Integer>	Read-only	Number of configured locations in the database file (static locations).
lines	<Integer>	Read-only	Number of lines in the databse files.
errors	<Integer>	Read-only	Number of errros encountered while

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			reading the database file.
warnings	<Integer>	Read-only	Number of warnings encountered while reading the database file.
entries	<Integer>	Read-only	Number of successfully added entries.
locationfile6	<String>	Read-only	Currently loaded location database file.
format6	<String>	Read-only	Location file format. Possible values = netscaler6, geoip-country6
custom6	<Integer>	Read-only	Number of configured custom locations.
static6	<Integer>	Read-only	Number of configured locations in the database file (static locations).
lines6	<Integer>	Read-only	Number of lines in the databse files.
errors6	<Integer>	Read-only	Number of errros encountered while reading the database file.
warnings6	<Integer>	Read-only	Number of warnings encountered while

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			reading the database file.
entries6	<Integer>	Read-only	Number of successfully added entries.
flags	<Integer>	Read-only	Information needed for display. This argument passes information from the kernel to the user space.
status	<Integer>	Read-only	This argument displays when the status (success or failure) of database loading.
databasemode	<String>	Read-only	This argument displays the database mode. Possible values = File, Internal, Not applicable
flushing	<String>	Read-only	This argument displays the state of flushing. Possible values = In progress, Idle
loading	<String>	Read-only	This argument displays the state of loading. Possible values = In progress, Idle
builtin	<String[]>	Read-only	.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL
feature	<String>	Read-only	The feature to be checked while applying this config.
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- UPDATE
- UNSET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/locationparameter **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"locationparameter":{

"context":<String_value>,

"q1label":<String_value>,

"q2label":<String_value>,

"q3label":<String_value>,

"q4label":<String_value>,

"q5label":<String_value>,

"q6label":<String_value>,

"matchwildcardtoany":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/locationparameter? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"locationparameter":{

"context":true,

"q1label":true,

"q2label":true,

"q3label":true,

"q4label":true,

"q5label":true,

"q6label":true,

"matchwildcardtoany":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/locationparameter **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "locationparameter": [ {

"context":<String_value>,

"q1label":<String_value>,

"q2label":<String_value>,

"q3label":<String_value>,

"q4label":<String_value>,

"q5label":<String_value>,

"q6label":<String_value>,

"Locationfile":<String_value>,

"format":<String_value>,

"custom":<Integer_value>,

"Static":<Integer_value>,

"lines":<Integer_value>,

"errors":<Integer_value>,

"warnings":<Integer_value>,
```

```
"entries":<Integer_value>,

"locationfile6":<String_value>,

"format6":<String_value>,

"custom6":<Integer_value>,

"static6":<Integer_value>,

"lines6":<Integer_value>,

"errors6":<Integer_value>,

"warnings6":<Integer_value>,

"entries6":<Integer_value>,

"flags":<Integer_value>,

"status":<Integer_value>,

"databasemode":<String_value>,

"flushing":<String_value>,

"loading":<String_value>,

"matchwildcardtoany":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

mcpprofile

Configuration for mcpProfile resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the mcp profile. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space ( ), at (@), equals (=), colon (:), and underscore characters. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my mcp profile").
proxymode	<String>	Read-write	Proxy mode for the MCP profile. FORWARD mode replaces Host and URL in backend requests. REVERSE mode passes requests as-is.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: FORWARD Possible values = FORWARD, REVERSE
profiletype	<String>	Read-write	Type of MCP profile. Frontend profiles apply to the entity that receives requests from a client. Backend profiles apply to the entity that sends client requests to a server. Default value: BACKEND Possible values = BACKEND, FRONTEND
hostreplacement	<String>	Read-write	Whether the Host header should be replaced with the backend MCP server FQDN in FORWARD proxy mode. If mcpProxyMode is FORWARD, this parameter is ENABLED bydefault. If mcpProxyMode is REVERSE, this parameter is DISABLED and cannot be ENABLED.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ENABLED, DISABLED
urlreplacement	<String>	Read-write	Whether the URL should be replaced with the backend MCP server URL in FORWARD proxy mode. If mcpProxyMode is FORWARD, this parameter is ENABLED bydefault. If mcpProxyMode is REVERSE, this parameter is DISABLED and cannot be ENABLED. Possible values = ENABLED, DISABLED
protocolversion	<String>	Read-write	MCP protocol version to advertise during monitoring of a mcp server.
tokenorapi	<String>	Read-write	If you like to insert Bearer or API token, configure this parameter with full header.
comment	<String>	Read-write	Any information about the MCP profile.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
insertheaderinclientrequest	<String>	Read-write	Whether mcp_token_or_api configuration will be used for MCP requests coming from client. Default value: DISABLED Possible values = ENABLED, DISABLED
newname	<String>	Read-write	New name for the mcpProfile. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Minimum length = 1
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- UPDATE
- UNSET

- DELETE
- GET (ALL)
- GET
- COUNT
- RENAME

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/mcpprofile **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"mcpprofile":{

<b>"name":<String_value>,

</b>"proxymode":<String_value>,

"profiletype":<String_value>,

"hostreplacement":<String_value>,

"urlreplacement":<String_value>,

"protocolversion":<String_value>,

"tokenorapi":<String_value>,

"comment":<String_value>,

"insertheaderinclientrequest":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/mcpprofile **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"mcpprofile":{

<b>"name":<String_value>,

</b>"proxymode":<String_value>,

"hostreplacement":<String_value>,

"urlreplacement":<String_value>,

"protocolversion":<String_value>,

"tokenorapi":<String_value>,

"comment":<String_value>,

"insertheaderinclientrequest":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/mcpprofile? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"mcpprofile":{

<b>"name":<String_value>,

</b>"proxymode":true,
```

```
"hostreplacement":true,

"urlreplacement":true,

"protocolversion":true,

"tokenorapi":true,

"comment":true,

"insertheaderinclientrequest":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/mcpprofile/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

RENAME

URL: http:// <netscaler-ip-address> /nitro/v1/config/mcpprofile? **action=rename HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"mcpprofile":{

<b>"name":<String_value>,

</b><b>"newname":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/mcpprofile **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/mcpprofile? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/mcpprofile? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of mcpprofile resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/mcpprofile? **view=summary**

Use this query-parameter to get the summary output of mcpprofile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/mcpprofile? **pagesize=#no;pageno=#no**

Use this query-parameter to get the mcpprofile resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "mcpprofile": [ {

"name":<String_value>,

"proxymode":<String_value>,

"profiletype":<String_value>,

"hostreplacement":<String_value>,

"urlreplacement":<String_value>,

"protocolversion":<String_value>,

"tokenorapi":<String_value>,

"comment":<String_value>,

"insertheaderinclientrequest":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/mcpprofile/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/mcpprofile/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/mcpprofile/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of mcpprofile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "mcpprofile": [ {

"name":<String_value>,

"proxymode":<String_value>,

"profiletype":<String_value>,

"hostreplacement":<String_value>,

"urlreplacement":<String_value>,

"protocolversion":<String_value>,

"tokenorapi":<String_value>,
```

```
"comment":<String_value>,

"insertheaderinclientrequest":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/mcpprofile? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "mcpprofile": [ { "__count": "#no"} ] }
```

nstrace

Configuration for nstrace operations resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
nf	<Integer>	Read-write	Number of files to be generated in cycle. Default value: 24 Minimum value = 1 Maximum value = 100
time	<Integer>	Read-write	Time per file (sec). Default value: 3600 Minimum value = 1
size	<Integer>	Read-write	Size of the captured data. Set 0 for full packet trace. Default value: 164 Minimum value = 0 Maximum value = 1514
mode	<String[]>	Read-write	Capturing mode for trace. Mode can be any of the following values or combination of these values: RX Received packets before NIC pipelining (Filter does not work when RX capturing mode is ON)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			NEW_RX Received packets after NIC pipelining TX Transmitted packets TXB Packets buffered for transmission IPV6 Translated IPv6 packets C2C Capture C2C message NS_FR_TX TX/TXB packets are not captured in flow receiver. MPTCP MPTCP master flow HTTP_QUIC HTTP-over-QUIC stream data and stream events Default mode: NEW_RX TXB . Default value: DEFAULT_MODE Possible values = TX, TXB, RX, IPV6, NEW_RX, C2C, NS_FR_TX,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			APPFW, MPTCP, PolicyBased, HTTP_QUIC
pernic	<String>	Read-write	Use separate trace files for each interface. Works only with cap format. Default value: DISABLED Possible values = ENABLED, DISABLED
filename	<String>	Read-write	Name of the trace file.
fileid	<String>	Read-write	ID for the trace file name for uniqueness. Should be used only with -name option.
filter	<String>	Read-write	Filter expression for nstrace. Maximum length of filter is 255 and it can be of following format: <expression> [<relop> <expression>] <relop> = (;; | ||) <expression> =: CONNECTION.<qualifier>.<qualifier-

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			method>.(<qualifier-value>) <qualifier> = SRCIP <qualifier-method> = [EQ | NE] <qualifier-value> = A valid IPv4 address. example = CONNECTION.SRCIP.EQ(127.0.0.1) <qualifier> = DSTIP <qualifier-method> = [EQ | NE] <qualifier-value> = A valid IPv4 address. example = CONNECTION.DSTIP.EQ(127.0.0.1) <qualifier> = IP <qualifier-method> = [EQ | NE] <qualifier-value> = A valid IPv4 address.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			example = CONNECTION.IP.EQ(127.0.0.1) <qualifier> = SRCIPv6 <qualifier-method> = [EQ | NE] <qualifier-value> = A valid IPv6 address. example = CONNECTION.SRCIPv6.EQ(2001:db8:0:0:1::1) <qualifier> = DSTIPv6 <qualifier-method> = [EQ | NE] <qualifier-value> = A valid IPv6 address. example = CONNECTION.DSTIPv6.EQ(2001:db8:0:0:1::1) <qualifier> = IPv6 <qualifier-method> = [EQ | NE]

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			<qualifier-value> = A valid IPv6 address. example = CONNECTION.IPv6.EQ(2001:db8:0:0:1::1) <qualifier> = SRCPORT <qualifier-method> = [EQ | NE | GT | GE | LT | LE | BETWEEN] <qualifier-value> = A valid port number. example = CONNECTION.SRCPORT.EQ(80) <qualifier> = DSTPORT <qualifier-method> = [EQ | NE | GT | GE | LT | LE | BETWEEN] <qualifier-value> = A valid port number.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			example = CONNECTION.DSTPORT.EQ(80) <qualifier> = PORT <qualifier-method> = [EQ | NE | GT | GE | LT | LE | BETWEEN] <qualifier-value> = A valid port number. example = CONNECTION.PORT.EQ(80) <qualifier> = VLANID <qualifier-method> = [EQ | NE | GT | GE | LT | LE | BETWEEN] <qualifier-value> = A valid VLAN ID. example = CONNECTION.VLANID.EQ(0) <qualifier> = CONNID

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			<qualifier-method> = [EQ | NE | GT | GE | LT | LE | BETWEEN] <qualifier-value> = A valid PCB dev number. example = CONNECTION.CONNID.EQ(0) <qualifier> = PPEID <qualifier-method> = [EQ | NE | GT | GE | LT | LE | BETWEEN] <qualifier-value> = A valid core ID. example = CONNECTION.PPEID.EQ(0) <qualifier> = SVCNAME <qualifier-method> = [EQ | NE | CONTAINS | STARTSWITH | ENDSWITH]

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			<qualifier-value> = A valid text string. example = CONNECTION.SVCNAME.EQ("name") <qualifier> = LB_VSERVER.NAME <qualifier-method> = [EQ | NE | CONTAINS | STARTSWITH | ENDSWITH] <qualifier-value> = LB vserver name. example = CONNECTION.LB_VSERVER.NAME.EQ("name") <qualifier> = CS_VSERVER.NAME <qualifier-method> = [EQ | NE | CONTAINS | STARTSWITH | ENDSWITH]

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			<qualifier-value> = CS vserver name. example = CONNECTION.CS_VSERVER.NAME.EQ("name") <qualifier> = INTF <qualifier-method> = [EQ | NE] <qualifier-value> = A valid interface id in the form of x/y. example = CONNECTION.INTF.EQ("x/y") <qualifier> = SERVICE_TYPE <qualifier-method> = [EQ | NE] <qualifier-value> = (SVC_HTTP | FTP | TCP | UDP | SSL | SSL_BRIDGE | SSL_TCP | NNTP | RPCSVR | RPCSVRS |

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			RPCCLNT | SVC_DNS | ADNS | SNMP | RTSP | DHCPRA | ANY| MONITOR | MONITOR_UDP | MONITOR_PING | SIP_UDP | SVC_MYSQL | SVC_MSSQL | FIX | SSL_FIX | PKTSTEER | SVC_AAA | SERVICE_UNKNOWN) example = CONNECTION.SERVICE_TYPE.EQ(ANY) <qualifier> = TRAFFIC_DOMAIN_ID <qualifier-method> = [EQ | NE | GT | GE | LT | LE | BETWEEN] <qualifier-value> = A valid traffic domain ID.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			example = CONNECTION.TRAFFIC_DOMAIN_ID.EQ(0) eg: start nstrace -filter "CONNECTION.SRCIP.EQ(127.0.0.1) || (CONNECTION.SVCNAME.NE("s1") ;; CONNECTION.SRCPORT.EQ(80))" The filter expression should be given in double quotes. common use cases: Trace capturing full sized traffic from/to ip 10.102.44.111, excluding loopback traffic start nstrace -size 0 -filter "CONNECTION.IP.NE(127.0.0.1) ;; CONNECTION.IP.EQ(10.102.44.111)" Trace capturing all traffic to (terminating at) port 80 or 443

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			start nstrace -size 0 -filter "CONNECTION.DSTPORT.EQ(443) || CONNECTION.DSTPORT.EQ(80)" Trace capturing all backend traffic specific to service service1 along with corresponding client side traffic start nstrace -size 0 -filter "CONNECTION.SVCNAME.EQ("service1")" -link ENABLED Trace capturing all traffic through NetScaler interface 1/1 start nstrace -filter "CONNECTION.INTF.EQ("1/1")" Trace capturing all traffic specific through vlan 2 start nstrace -filter "CONNECTION.VLANID.EQ(2)"

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Trace capturing all frontend (client side) traffic specific to lb vserver vserver1 along with corresponding server side traffic start nstrace -size 0 -filter "CONNECTION.LB_VSERVER.NAME.EQ("vserver1")" -link ENABLED .
link	<String>	Read-write	Includes filtered connection's peer traffic. Default value: DISABLED Possible values = ENABLED, DISABLED
nodes	<Integer[]>	Read-write	Nodes on which tracing is started. Minimum value = 0 Maximum value = 32
filesize	<Integer>	Read-write	File size, in MB, treshold for rollover. If free disk space is less than 2GB at the time of rollover, trace will stop

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			. Default value: 1024 Minimum value = 0 Maximum value = 10240
traceformat	<String>	Read-write	Format in which trace will be generated . Default value: 0 Possible values = NSCAP, PCAP
merge	<String>	Read-write	Specify how traces across PE's are merged . Default value: 0 Possible values = ONSTOP, ONTHEFLY, NOMERGE
doruntimecleanup	<String>	Read-write	Enable or disable runtime temp file cleanup. Default value: ENABLED Possible values = ENABLED, DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
tracebuffers	<Integer>	Read-write	Number of 16KB trace buffers. Default value: 5000 Minimum value = 1000
skiprpc	<String>	Read-write	skip RPC packets. Default value: DISABLED Possible values = ENABLED, DISABLED
skiplocalssh	<String>	Read-write	skip local SSH packets. Default value: DISABLED Possible values = ENABLED, DISABLED
capsslkeys	<String>	Read-write	Capture SSL Master keys. Master keys will not be captured on FIPS machine. Warning: The captured keys can be used to decrypt information that may be confidential. The captured key files have to be stored in a secure environment.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: DISABLED Possible values = ENABLED, DISABLED
capdroppkt	<String>	Read-write	Captures Dropped Packets if set to ENABLED. Default value: DISABLED Possible values = ENABLED, DISABLED
inmemorytrace	<String>	Read-write	Logs packets in appliance's memory and dumps the trace file on stopping the nstrace operation. Default value: DISABLED Possible values = ENABLED, DISABLED
nodeid	<Integer>	Read-write	Unique number that identifies the cluster node. Minimum value = 0 Maximum value = 31
state	<String>	Read-only	Current running state of trace.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: 0 Possible values = RUNNING, STOPPED
scope	<String>	Read-only	Scope of started trace, local or cluster level. Default value: 0 Possible values = CLUSTER, LOCAL
tracelocation	<String>	Read-only	Directory where current trace files are saved.
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- START
- STOP
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of

creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

START

URL: http:// <netscaler-ip-address> /nitro/v1/config/nstrace? **action=start HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nstrace":{

"nf":<Integer_value>,

"time":<Integer_value>,

"size":<Integer_value>,

"mode":<String[]_value>,

"pernic":<String_value>,

"filename":<String_value>,

"fileid":<String_value>,

"filter":<String_value>,
```

```
"link":<String_value>,

"nodes":<Integer[]_value>,

"filesize":<Integer_value>,

"traceformat":<String_value>,

"merge":<String_value>,

"doruntimecleanup":<String_value>,

"tracebuffers":<Integer_value>,

"skiprpc":<String_value>,

"skiplocalssh":<String_value>,

"capsslkeys":<String_value>,

"capdroppkt":<String_value>,

"inmemorytrace":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

STOP

URL: http:// <netscaler-ip-address> /nitro/v1/config/nstrace? **action=stop HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nstrace":{

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/nstrace **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/nstrace? **args=nodeid: <Integer_value>**

Use this query-parameter to get nstrace resources based on additional properties.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nstrace": [ {

nodeid:<Integer_value>"state":<String_value>,

"scope":<String_value>,

"tracelocation":<String_value>,

"nf":<Integer_value>,
```

```
"time":<Integer_value>,

"size":<Integer_value>,

"mode":<String[]_value>,

"traceformat":<String_value>,

"pernic":<String_value>,

"filename":<String_value>,

"fileid":<String_value>,

"filter":<String_value>,

"link":<String_value>,

"nodes":<Integer[]_value>,

"merge":<String_value>,

"doruntimecleanup":<String_value>,

"tracebuffers":<Integer_value>,

"skiprpc":<String_value>,

"skiplocalssh":<String_value>,

"capsslkeys":<String_value>,

"capdroppkt":<String_value>,

"inmemorytrace":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

radiusnode

Configuration for RADIUS Node resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
nodeprefix	<String>	Read-write	IP address/IP prefix of radius node in CIDR format.
radkey	<String>	Read-write	The key shared between the RADIUS server and clients. Required for NetScaler to communicate with the RADIUS nodes.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- UPDATE
- DELETE
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/radiusnode **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"radiusnode":{

<b>"nodeprefix":<String_value>,

</b><b>"radkey":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/radiusnode **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"radiusnode":{

<b>"nodeprefix":<String_value>,

</b>"radkey":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/radiusnode/ nodeprefix_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/radiusnode **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/radiusnode? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/radiusnode? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of radiusnode resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/radiusnode? **view=summary**

Use this query-parameter to get the summary output of radiusnode resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/radiusnode? **pagesize=#no;pageno=#no**

Use this query-parameter to get the radiusnode resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "radiusnode": [ {

"nodeprefix":<String_value>,

"radkey":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/radiusnode/ nodeprefix_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/radiusnode/ nodeprefix_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/radiusnode/ nodeprefix_value<String> ? **view=summary**

Use this query-parameter to get the summary output of radiusnode resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "radiusnode": [ {

"nodeprefix":<String_value>,

"radkey":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/radiusnode? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "radiusnode": [ { "__count": "#no"} ] }
```

server

Configuration for server resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the server. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Can be changed after the name is created. Minimum length = 1
ipaddress	<String>	Read-write	IPv4 or IPv6 address of the server. If you create an IP address based server, you can specify the name of the server, instead of its IP address, when creating a service. Note: If you do not create a server entry, the server IP address that you enter when you create a service becomes the name of the server.
domain	<String>	Read-write	Domain name of the server. For a domain

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			based configuration, you must create the server first. Minimum length = 1
translationip	<String>	Read-write	IP address used to transform the server's DNS-resolved IP address.
translationmask	<String>	Read-write	The netmask of the translation ip.
domainresolveretry	<Integer>	Read-write	Time, in seconds, for which the NetScaler must wait, after DNS resolution fails, before sending the next DNS query to resolve the domain name. Default value: 5 Minimum value = 5 Maximum value = 20939
state	<String>	Read-write	Initial state of the server. Default value: ENABLED Possible values = ENABLED, DISABLED
ipv6address	<String>	Read-write	Support IPv6 addressing mode. If you configure a server with the IPv6

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			addressing mode, you cannot use the server in the IPv4 addressing mode. Default value: NO Possible values = YES, NO
comment	<String>	Read-write	Any information about the server.
td	<Integer>	Read-write	Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0. Minimum value = 0 Maximum value = 4094
querytype	<String>	Read-write	Specify the type of DNS resolution to be done on the configured domain to get the backend services. Valid query types are A, AAAA and SRV with A being the default querytype. The type of DNS resolution done on the domains in SRV records is

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			inherited from ipv6 argument. Default value: A Possible values = A, AAAA, SRV
domainresolvenow	<Boolean>	Read-write	Immediately send a DNS query to resolve the server's domain name.
delay	<Integer>	Read-write	Time, in seconds, after which all the services configured on the server are disabled.
graceful	<String>	Read-write	Shut down gracefully, without accepting any new connections, and disabling each service when all of its connections are closed. Default value: NO Possible values = YES, NO
Internal	<Boolean>	Read-write	Display names of the servers that have been created for internal use.
newname	<String>	Read-write	New name for the server. Must begin with an ASCII alphabetic or underscore (_)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Minimum length = 1
statechangetimesec	<String>	Read-only	Time when last state change happened. Seconds part.
tickssincelaststatechange	<Integer>	Read-only	Time in 10 millisecond ticks since the last state change.
autoscale	<String>	Read-only	Auto scale option for a servicegroup. Default value: DISABLED Possible values = DISABLED, DNS, POLICY, CLOUD, API
usip	<String>	Read-only	Use the client's IP address as the source IP address when initiating a connection to the server. When creating a service, if you do not set this parameter, the service inherits the global Use Source IP

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			setting (available in the enable ns mode and disable ns mode CLI commands, or in the System > Settings > Configure modes > Configure Modes dialog box). However, you can override this setting after you create the service. Possible values = YES, NO
cka	<String>	Read-only	Enable client keep-alive for the service group. Possible values = YES, NO
tcpb	<String>	Read-only	Enable TCP buffering for the service group. Possible values = YES, NO
cmp	<String>	Read-only	Enable compression for the specified service. Possible values = YES, NO
cacheable	<String>	Read-only	Use the transparent cache redirection virtual server to forward the request to the cache server. Default value: NO

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = YES, NO
sp	<String>	Read-only	Enable surge protection for the service group. Default value: OFF Possible values = ON, OFF
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- ENABLE
- DISABLE
- GET (ALL)
- GET
- COUNT
- RENAME

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/server **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"server":{

<b>"name":<String_value>,

</b>"ipaddress":<String_value>,

"domain":<String_value>,

"translationip":<String_value>,

"translationmask":<String_value>,

"domainresolveretry":<Integer_value>,
```

```
"state":<String_value>,

"ipv6address":<String_value>,

"comment":<String_value>,

"td":<Integer_value>,

"querytype":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/server/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/server **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"server":{

<b>"name":<String_value>,

</b>"ipaddress":<String_value>,

"domainresolveretry":<Integer_value>,

"translationip":<String_value>,

"translationmask":<String_value>,

"domainresolvenow":<Boolean_value>,

"comment":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/server? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"server":{

<b>"name":<String_value>,

</b>"comment":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

ENABLE

URL: http:// <netscaler-ip-address> /nitro/v1/config/server? **action=enable HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"server":{

<b>"name":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DISABLE

URL: http:// <netscaler-ip-address> /nitro/v1/config/server? **action=disable HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"server":{

<b>"name":<String_value>,

</b>"delay":<Integer_value>,

"graceful":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

RENAME

URL: http:// <netscaler-ip-address> /nitro/v1/config/server? **action=rename HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"server":{

<b>"name":<String_value>,

</b><b>"newname":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/server **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/server? **args=name: <String_value> ,Internal: <Boolean_value> ,ipaddress: <String_value> ,domain: <String_value>**

Use this query-parameter to get server resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/config/server? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/server? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of server resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/server? **view=summary**

Use this query-parameter to get the summary output of server resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/server? **pagesize=#no;pageno=#no**

Use this query-parameter to get the server resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "server": [ {

name:<String_value>,Internal:<Boolean_value>,ipaddress:<String_value>,doma
in:<String_value>"ipaddress":<String_value>,

"state":<String_value>,

"domain":<String_value>,

"domainresolveretry":<Integer_value>,

"translationip":<String_value>,

"translationmask":<String_value>,

"comment":<String_value>,

"statechangetimesec":<String_value>,

"tickssincelaststatechange":<Integer_value>,

"ipv6address":<String_value>,

"td":<Integer_value>,

"autoscale":<String_value>,

"usip":<String_value>,

"cka":<String_value>,

"tcpb":<String_value>,

"cmp":<String_value>,

"cacheable":<String_value>,

"sp":<String_value>,

"querytype":<String_value>,
```

```
"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/server/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/server/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/server/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of server resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "server": [ {

name:<String_value>,Internal:<Boolean_value>,ipaddress:<String_value>,doma
in:<String_value>"ipaddress":<String_value>,

"state":<String_value>,
```

```
"domain":<String_value>,

"domainresolveretry":<Integer_value>,

"translationip":<String_value>,

"translationmask":<String_value>,

"comment":<String_value>,

"statechangetimesec":<String_value>,

"tickssincelaststatechange":<Integer_value>,

"ipv6address":<String_value>,

"td":<Integer_value>,

"autoscale":<String_value>,

"usip":<String_value>,

"cka":<String_value>,

"tcpb":<String_value>,

"cmp":<String_value>,

"cacheable":<String_value>,

"sp":<String_value>,

"querytype":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/server? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "server": [ { "__count": "#no"} ] }
```

server_binding

Binding object which returns the resources bound to server.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the server for which to display parameters. Minimum length = 1
server_servicegroup_binding	<server_servicegroup_binding[]>	Read-only	servicegroup that can be bound to server.
server_gslbservice_binding	<server_gslbservice_binding[]>	Read-only	gslbservice that can be bound to server.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
server_gslbservicegroup_binding	<server_gslbservicegroup_binding[]>	Read-only	gslbservicegroup that can be bound to server.
server_service_binding	<server_service_binding[]>	Read-only	service that can be bound to server.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/server_binding/ name_value<String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "server_binding": [ {

"name":<String_value>,

"server_gslbservice_binding":<server_gslbservice_binding[]_value>,

"server_service_binding":<server_service_binding[]_value>,

"server_servicegroup_binding":<server_servicegroup_binding[]_value>,

"server_gslbservicegroup_binding":<server_gslbservicegroup_binding[]_value
>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/server_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/server_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "server_binding": [ {

"name":<String_value>,

"server_gslbservice_binding":<server_gslbservice_binding[]_value>,

"server_service_binding":<server_service_binding[]_value>,

"server_servicegroup_binding":<server_servicegroup_binding[]_value>,

"server_gslbservicegroup_binding":<server_gslbservicegroup_binding[]_value
>

}]}
```

server_gslbservice_binding

Binding object showing the gslbservice that can be bound to server.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
servicename	<String>	Read-write	The services attatched to the server.
name	<String>	Read-write	Name of the server for which to display parameters. Minimum length = 1
svctype	<String>	Read-only	The type of bound service. Possible values = HTTP, FTP, TCP, UDP, SSL, SSL_BRIDGE, SSL_TCP, DTLS, NNTP, RPCSVR, DNS, ADNS, SNMP, RTSP, DHCPRA, ANY, SIP_UDP, SIP_TCP, SIP_SSL, DNS_TCP, ADNS_TCP, MYSQL, MSSQL, ORACLE, MONGO, MONGO_TLS, RADIUS, RADIUSListener, RDP, DIAMETER, SSL_DIAMETER, TFTP, SMPP, PPTP, GRE, SYSLOGTCP, SYSLOGUDP, FIX, SSL_FIX, USER_TCP, USER_SSL_TCP, QUIC, IPFIX,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			LOGSTREAM, LOGSTREAM_SSL, MQTT, MQTT_TLS, QUIC_BRIDGE, DOT, ADNS_DOT, HTTP_QUIC, ADNS_DOH, KAFKA_BROKER
port	<Integer>	Read-only	The port number to be used for the bound service. Range 1 - 65535 * in CLI is represented as 65535 in NITRO API
serviceipaddress	<String>	Read-only	The IP address of the bound service.
serviceipstr	<String>	Read-only	This field has been intorduced to show the dbs services ip.
svrstate	<String>	Read-only	The state of the bound service. Possible values = UP, DOWN, UNKNOWN, BUSY, OUT OF SERVICE, GOING OUT OF SERVICE, DOWN WHEN GOING OUT OF SERVICE, NS_EMPTY_STR,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Unknown, DISABLED
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/server_gslbservice_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ server_gslbservice_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of server_gslbservice_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/server_gslbservice_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the server_gslbservice_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "server_gslbservice_binding": [ {

"servicename":<String_value>,

"name":<String_value>,

"svctype":<String_value>,

"port":<Integer_value>,

"serviceipaddress":<String_value>,
```

```
"serviceipstr":<String_value>,

"svrstate":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/server_gslbservice_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/server_gslbservice_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "server_gslbservice_binding": [ {

"servicename":<String_value>,

"name":<String_value>,

"svctype":<String_value>,
```

```
"port":<Integer_value>,

"serviceipaddress":<String_value>,

"serviceipstr":<String_value>,

"svrstate":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/server_gslbservice_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"server_gslbservice_binding": [ { "__count": "#no"} ] }
```

server_gslbservicegroup_binding

Binding object showing the gslbservicegroup that can be bound to server.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the server for which to display parameters. Minimum length = 1
servicegroupname	<String>	Read-write	servicegroups bind to this server.
dup_svctype	<String>	Read-only	service type of the service. Possible values = HTTP, FTP, TCP, UDP, SSL, SSL_BRIDGE, SSL_TCP, DTLS, NNTP, RPCSVR, DNS, ADNS, SNMP, RTSP, DHCPRA, ANY, SIP_UDP, SIP_TCP, SIP_SSL, DNS_TCP, ADNS_TCP, MYSQL, MSSQL, ORACLE, MONGO, MONGO_TLS, RADIUS, RADIUSListener, RDP, DIAMETER, SSL_DIAMETER, TFTP, SMPP, PPTP, GRE, SYSLOGTCP, SYSLOGUDP, FIX, SSL_FIX, USER_TCP, USER_SSL_TCP, QUIC, IPFIX, LOGSTREAM,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			LOGSTREAM_SSL, MQTT, MQTT_TLS, QUIC_BRIDGE, DOT, ADNS_DOT, HTTP_QUIC, ADNS_DOH, KAFKA_BROKER
monthreshold	<Integer>	Read-only	Minimum sum of weights of the monitors that are bound to this service. Used to determine whether to mark a service as UP or DOWN. Minimum value = 0 Maximum value = 65535
clttimeout	<Integer>	Read-only	Time, in seconds, after which to terminate an idle client connection. Minimum value = 0 Maximum value = 31536000
cipheader	<String>	Read-only	Name of the HTTP header whose value must be set to the IP address of the client. Used with the Client IP parameter. If client IP insertion is enabled, and the client IP header is not specified, the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			value of Client IP Header parameter or the value set by the set ns config command is used as client's IP header name. Minimum length = 1
maxbandwidth	<Integer>	Read-only	Maximum bandwidth, in Kbps, allocated for all the services in the service group. Minimum value = 0 Maximum value = 4294967287
customserverid	<String>	Read-only	A positive integer to identify the service. Used when the persistency type is set to Custom Server ID. Default value: "None"
dup_port	<Integer>	Read-only	port of the service. Range 1 - 65535 * in CLI is represented as 65535 in NITRO API
cip	<String>	Read-only	Before forwarding a request to the service, insert an HTTP header with the client's IPv4 or IPv6 address as its

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			value. Used if the server needs the client's IP address for security, accounting, or other purposes, and setting the Use Source IP parameter is not a viable option. Possible values = ENABLED, DISABLED
svctype	<String>	Read-only	The type of bound service. Possible values = HTTP, FTP, TCP, UDP, SSL, SSL_BRIDGE, SSL_TCP, DTLS, NNTP, RPCSVR, DNS, ADNS, SNMP, RTSP, DHCPRA, ANY, SIP_UDP, SIP_TCP, SIP_SSL, DNS_TCP, ADNS_TCP, MYSQL, MSSQL, ORACLE, MONGO, MONGO_TLS, RADIUS, RADIUSListener, RDP, DIAMETER, SSL_DIAMETER, TFTP, SMPP, PPTP, GRE, SYSLOGTCP, SYSLOGUDP, FIX,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			SSL_FIX, USER_TCP, USER_SSL_TCP, QUIC, IPFIX, LOGSTREAM, LOGSTREAM_SSL, MQTT, MQTT_TLS, QUIC_BRIDGE, DOT, ADNS_DOT, HTTP_QUIC, ADNS_DOH, KAFKA_BROKER
port	<Integer>	Read-only	The port number to be used for the bound service. Range 1 - 65535 * in CLI is represented as 65535 in NITRO API
serviceipstr	<String>	Read-only	This field has been intorduced to show the dbs services ip.
boundtd	<Integer>	Read-only	Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum value = 0 Maximum value = 4094
serviceipaddress	<String>	Read-only	The IP address of the bound service.
downstateflush	<String>	Read-only	Perform delayed clean-up of connections to all services in the service group. Default value: ENABLED Possible values = ENABLED, DISABLED
svrcfgflags	<Integer>	Read-only	service flags to denote its a db enabled.
maxclient	<Integer>	Read-only	Maximum number of simultaneous open connections for the service group. Minimum value = 0 Maximum value = 4294967294
maxreq	<Integer>	Read-only	Maximum number of requests that can be sent on a persistent connection to the service group. Note: Connection requests beyond this value are rejected.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum value = 0 Maximum value = 65535
appflowlog	<String>	Read-only	Enable logging of AppFlow information for the specified service group. Default value: ENABLED Possible values = ENABLED, DISABLED
svrstate	<String>	Read-only	The state of the bound service. Possible values = UP, DOWN, UNKNOWN, BUSY, OUT OF SERVICE, GOING OUT OF SERVICE, DOWN WHEN GOING OUT OF SERVICE, NS_EMPTY_STR, Unknown, DISABLED
svrtimeout	<Integer>	Read-only	Time, in seconds, after which to terminate an idle server connection. Minimum value = 0 Maximum value = 31536000

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/server_gslbservicegroup_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ server_gslbservicegroup_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of server_gslbservicegroup_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/server_gslbservicegroup_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the server_gslbservicegroup_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "server_gslbservicegroup_binding": [ {

"name":<String_value>,

"servicegroupname":<String_value>,

"dup_svctype":<String_value>,

"monthreshold":<Integer_value>,

"clttimeout":<Integer_value>,
```

```
"cipheader":<String_value>,

"maxbandwidth":<Integer_value>,

"customserverid":<String_value>,

"dup_port":<Integer_value>,

"cip":<String_value>,

"svctype":<String_value>,

"port":<Integer_value>,

"serviceipstr":<String_value>,

"boundtd":<Integer_value>,

"serviceipaddress":<String_value>,

"downstateflush":<String_value>,

"svrcfgflags":<Integer_value>,

"maxclient":<Integer_value>,

"maxreq":<Integer_value>,

"appflowlog":<String_value>,

"svrstate":<String_value>,

"svrtimeout":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/server_gslbservicegroup_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/server_gslbservicegroup_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "server_gslbservicegroup_binding": [ {

"name":<String_value>,

"servicegroupname":<String_value>,

"dup_svctype":<String_value>,

"monthreshold":<Integer_value>,

"clttimeout":<Integer_value>,

"cipheader":<String_value>,

"maxbandwidth":<Integer_value>,

"customserverid":<String_value>,

"dup_port":<Integer_value>,

"cip":<String_value>,
```

```
"svctype":<String_value>,

"port":<Integer_value>,

"serviceipstr":<String_value>,

"boundtd":<Integer_value>,

"serviceipaddress":<String_value>,

"downstateflush":<String_value>,

"svrcfgflags":<Integer_value>,

"maxclient":<Integer_value>,

"maxreq":<Integer_value>,

"appflowlog":<String_value>,

"svrstate":<String_value>,

"svrtimeout":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/server_gslbservicegroup_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"server_gslbservicegroup_binding": [ { "__count": "#no"} ] }
```

server_service_binding

Binding object showing the service that can be bound to server.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
servicename	<String>	Read-write	The services attatched to the server.
name	<String>	Read-write	Name of the server for which to display parameters. Minimum length = 1
port	<Integer>	Read-only	The port number to be used for the bound service. Range 1 - 65535 * in CLI is represented as 65535 in NITRO API
svctype	<String>	Read-only	The type of bound service. Possible values = HTTP, FTP, TCP, UDP, SSL, SSL_BRIDGE,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			SSL_TCP, DTLS, NNTP, RPCSVR, DNS, ADNS, SNMP, RTSP, DHCPRA, ANY, SIP_UDP, SIP_TCP, SIP_SSL, DNS_TCP, ADNS_TCP, MYSQL, MSSQL, ORACLE, MONGO, MONGO_TLS, RADIUS, RADIUSListener, RDP, DIAMETER, SSL_DIAMETER, TFTP, SMPP, PPTP, GRE, SYSLOGTCP, SYSLOGUDP, FIX, SSL_FIX, USER_TCP, USER_SSL_TCP, QUIC, IPFIX, LOGSTREAM, LOGSTREAM_SSL, MQTT, MQTT_TLS, QUIC_BRIDGE, DOT, ADNS_DOT, HTTP_QUIC, ADNS_DOH, KAFKA_BROKER
svrstate	<String>	Read-only	The state of the bound service. Possible values = UP, DOWN, UNKNOWN, BUSY,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			OUT OF SERVICE, GOING OUT OF SERVICE, DOWN WHEN GOING OUT OF SERVICE, NS_EMPTY_STR, Unknown, DISABLED
serviceipaddress	<String>	Read-only	The IP address of the bound service.
serviceipstr	<String>	Read-only	This field has been intorduced to show the dbs services ip.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of

creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/server_service_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/server_service_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of server_service_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/server_service_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the server_service_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "server_service_binding": [ {

"servicename":<String_value>,

"name":<String_value>,

"port":<Integer_value>,

"svctype":<String_value>,

"svrstate":<String_value>,

"serviceipaddress":<String_value>,

"serviceipstr":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/server_service_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/server_service_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "server_service_binding": [ {

"servicename":<String_value>,

"name":<String_value>,

"port":<Integer_value>,

"svctype":<String_value>,

"svrstate":<String_value>,

"serviceipaddress":<String_value>,

"serviceipstr":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/server_service_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"server_service_binding": [ { "__count": "#no"} ] }
```

server_servicegroup_binding

Binding object showing the servicegroup that can be bound to server.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the server for which to display parameters. Minimum length = 1
servicegroupname	<String>	Read-write	servicegroups bind to this server.
svrtimeout	<Integer>	Read-only	Time, in seconds, after which to terminate an idle server connection. Minimum value = 0 Maximum value = 31536000
appflowlog	<String>	Read-only	Enable logging of AppFlow information for the specified service group. Default value: ENABLED Possible values = ENABLED, DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
maxreq	<Integer>	Read-only	Maximum number of requests that can be sent on a persistent connection to the service group. Note: Connection requests beyond this value are rejected. Minimum value = 0 Maximum value = 65535
svcitmboundsvcs	<Integer>	Read-only	Indicates the total number of bound IPs for the SRV target FQDN.
svrstate	<String>	Read-only	The state of the bound service. Possible values = UP, DOWN, UNKNOWN, BUSY, OUT OF SERVICE, GOING OUT OF SERVICE, DOWN WHEN GOING OUT OF SERVICE, NS_EMPTY_STR, Unknown, DISABLED
usip	<String>	Read-only	Use the client's IP address as the source IP address when initiating a connection to the server. When creating a service, if

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			you do not set this parameter, the service inherits the global Use Source IP setting (available in the enable ns mode and disable ns mode CLI commands, or in the System > Settings > Configure modes > Configure Modes dialog box). However, you can override this setting after you create the service. Possible values = YES, NO
maxclient	<Integer>	Read-only	Maximum number of simultaneous open connections for the service group. Minimum value = 0 Maximum value = 4294967294
svrcfgflags	<Integer>	Read-only	service flags to denote its a db enabled.
svcitmactsvcs	<Integer>	Read-only	Indicates the total number of active IPs for SRV target FQDN.
tcpb	<String>	Read-only	Enable TCP buffering for the service group.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = YES, NO
sp	<String>	Read-only	Enable surge protection for the service group. Default value: OFF Possible values = ON, OFF
downstateflush	<String>	Read-only	Perform delayed clean-up of connections to all services in the service group. Default value: ENABLED Possible values = ENABLED, DISABLED
weight	<Integer>	Read-only	Indicates the weight of bound IPs.
svcitmpriority	<Integer>	Read-only	Indicates the Priority of the SRV target FQDN.
serviceipaddress	<String>	Read-only	The IP address of the bound service.
serviceipstr	<String>	Read-only	This field has been intorduced to show the dbs services ip.
boundtd	<Integer>	Read-only	Integer value that uniquely identifies the traffic domain in which you want to

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0. Minimum value = 0 Maximum value = 4094
port	<Integer>	Read-only	The port number to be used for the bound service. Range 1 - 65535 * in CLI is represented as 65535 in NITRO API
servicegroupentname2	<String>	Read-only	Used for show server of SRV type to indicate target FQDNs.
svctype	<String>	Read-only	The type of bound service. Possible values = HTTP, FTP, TCP, UDP, SSL, SSL_BRIDGE, SSL_TCP, DTLS, NNTP, RPCSVR, DNS, ADNS, SNMP, RTSP, DHCPRA, ANY, SIP_UDP, SIP_TCP, SIP_SSL,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			DNS_TCP, ADNS_TCP, MYSQL, MSSQL, ORACLE, MONGO, MONGO_TLS, RADIUS, RADIUSListener, RDP, DIAMETER, SSL_DIAMETER, TFTP, SMPP, PPTP, GRE, SYSLOGTCP, SYSLOGUDP, FIX, SSL_FIX, USER_TCP, USER_SSL_TCP, QUIC, IPFIX, LOGSTREAM, LOGSTREAM_SSL, MQTT, MQTT_TLS, QUIC_BRIDGE, DOT, ADNS_DOT, HTTP_QUIC, ADNS_DOH, KAFKA_BROKER
cmp	<String>	Read-only	Enable compression for the specified service. Possible values = YES, NO
dup_port	<Integer>	Read-only	port of the service. Range 1 - 65535 * in CLI is represented as

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			65535 in NITRO API
cip	<String>	Read-only	Before forwarding a request to the service, insert an HTTP header with the client's IPv4 or IPv6 address as its value. Used if the server needs the client's IP address for security, accounting, or other purposes, and setting the Use Source IP parameter is not a viable option. Possible values = ENABLED, DISABLED
customserverid	<String>	Read-only	A positive integer to identify the service. Used when the persistency type is set to Custom Server ID. Default value: "None"
maxbandwidth	<Integer>	Read-only	Maximum bandwidth, in Kbps, allocated for all the services in the service group. Minimum value = 0 Maximum value = 4294967287

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
cka	<String>	Read-only	Enable client keep-alive for the service group. Possible values = YES, NO
cipheader	<String>	Read-only	Name of the HTTP header whose value must be set to the IP address of the client. Used with the Client IP parameter. If client IP insertion is enabled, and the client IP header is not specified, the value of Client IP Header parameter or the value set by the set ns config command is used as client's IP header name. Minimum length = 1
cacheable	<String>	Read-only	Use the transparent cache redirection virtual server to forward the request to the cache server. Default value: NO Possible values = YES, NO
monthreshold	<Integer>	Read-only	Minimum sum of weights of the monitors that are bound to this service. Used to determine

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			whether to mark a service as UP or DOWN. Minimum value = 0 Maximum value = 65535
clttimeout	<Integer>	Read-only	Time, in seconds, after which to terminate an idle client connection. Minimum value = 0 Maximum value = 31536000
dup_svctype	<String>	Read-only	service type of the service. Possible values = HTTP, FTP, TCP, UDP, SSL, SSL_BRIDGE, SSL_TCP, DTLS, NNTP, RPCSVR, DNS, ADNS, SNMP, RTSP, DHCPRA, ANY, SIP_UDP, SIP_TCP, SIP_SSL, DNS_TCP, ADNS_TCP, MYSQL, MSSQL, ORACLE, MONGO, MONGO_TLS, RADIUS, RADIUSListener, RDP, DIAMETER, SSL_DIAMETER,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			TFTP, SMPP, PPTP, GRE, SYSLOGTCP, SYSLOGUDP, FIX, SSL_FIX, USER_TCP, USER_SSL_TCP, QUIC, IPFIX, LOGSTREAM, LOGSTREAM_SSL, MQTT, MQTT_TLS, QUIC_BRIDGE, DOT, ADNS_DOT, HTTP_QUIC, ADNS_DOH, KAFKA_BROKER
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of

creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/server_servicegroup_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ server_servicegroup_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of server_servicegroup_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/server_servicegroup_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the server_servicegroup_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "server_servicegroup_binding": [ {

"name":<String_value>,

"servicegroupname":<String_value>,

"svrtimeout":<Integer_value>,

"appflowlog":<String_value>,

"maxreq":<Integer_value>,

"svcitmboundsvcs":<Integer_value>,

"svrstate":<String_value>,

"usip":<String_value>,

"maxclient":<Integer_value>,

"svrcfgflags":<Integer_value>,

"svcitmactsvcs":<Integer_value>,

"tcpb":<String_value>,

"sp":<String_value>,

"downstateflush":<String_value>,

"weight":<Integer_value>,

"svcitmpriority":<Integer_value>,

"serviceipaddress":<String_value>,

"serviceipstr":<String_value>,

"boundtd":<Integer_value>,
```

```
"port":<Integer_value>,

"servicegroupentname2":<String_value>,

"svctype":<String_value>,

"cmp":<String_value>,

"dup_port":<Integer_value>,

"cip":<String_value>,

"customserverid":<String_value>,

"maxbandwidth":<Integer_value>,

"cka":<String_value>,

"cipheader":<String_value>,

"cacheable":<String_value>,

"monthreshold":<Integer_value>,

"clttimeout":<Integer_value>,

"dup_svctype":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/server_servicegroup_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ server_servicegroup_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "server_servicegroup_binding": [ {

"name":<String_value>,

"servicegroupname":<String_value>,

"svrtimeout":<Integer_value>,

"appflowlog":<String_value>,

"maxreq":<Integer_value>,

"svcitmboundsvcs":<Integer_value>,

"svrstate":<String_value>,

"usip":<String_value>,

"maxclient":<Integer_value>,

"svrcfgflags":<Integer_value>,

"svcitmactsvcs":<Integer_value>,

"tcpb":<String_value>,
```

```
"sp":<String_value>,

"downstateflush":<String_value>,

"weight":<Integer_value>,

"svcitmpriority":<Integer_value>,

"serviceipaddress":<String_value>,

"serviceipstr":<String_value>,

"boundtd":<Integer_value>,

"port":<Integer_value>,

"servicegroupentname2":<String_value>,

"svctype":<String_value>,

"cmp":<String_value>,

"dup_port":<Integer_value>,

"cip":<String_value>,

"customserverid":<String_value>,

"maxbandwidth":<Integer_value>,

"cka":<String_value>,

"cipheader":<String_value>,

"cacheable":<String_value>,

"monthreshold":<Integer_value>,

"clttimeout":<Integer_value>,

"dup_svctype":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/server_servicegroup_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"server_servicegroup_binding": [ { "__count": "#no"} ] }
```

service

Configuration for service resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the service. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the service has been created. Minimum length = 1
ip	<String>	Read-write	IP to assign to the service. Minimum length = 1
servername	<String>	Read-write	Name of the server that hosts the service. Minimum length = 1
servicetype	<String>	Read-write	Protocol in which data is exchanged with the service. Possible values = HTTP, FTP, TCP, UDP, SSL, SSL_BRIDGE, SSL_TCP, DTLS, NNTP, RPCSVR, DNS, ADNS, SNMP, RTSP, DHCPRA, ANY, SIP_UDP, SIP_TCP, SIP_SSL, DNS_TCP, ADNS_TCP, MYSQL, MSSQL, ORACLE, MONGO, MONGO_TLS, RADIUS,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			RADIUSListener, RDP, DIAMETER, SSL_DIAMETER, TFTP, SMPP, PPTP, GRE, SYSLOGTCP, SYSLOGUDP, FIX, SSL_FIX, USER_TCP, USER_SSL_TCP, QUIC, IPFIX, LOGSTREAM, LOGSTREAM_SSL, MQTT, MQTT_TLS, QUIC_BRIDGE, DOT, ADNS_DOT, HTTP_QUIC, ADNS_DOH, KAFKA_BROKER
port	<Integer>	Read-write	Port number of the service. Range 1 - 65535 * in CLI is represented as 65535 in NITRO API
cleartextport	<Integer>	Read-write	Port to which clear text data must be sent after the appliance decrypts incoming SSL traffic. Applicable to transparent SSL services. Minimum value = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
cachetype	<String>	Read-write	Cache type supported by the cache server. Possible values = TRANSPARENT, REVERSE, FORWARD
maxclient	<Integer>	Read-write	Maximum number of simultaneous open connections to the service. Minimum value = 0 Maximum value = 4294967294
healthmonitor	<String>	Read-write	Monitor the health of this service. Available settings function as follows: YES - Send probes to check the health of the service. NO - Do not send probes to check the health of the service. With the NO option, the appliance shows the service as UP at all times. Default value: YES Possible values = YES, NO

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
maxreq	<Integer>	Read-write	Maximum number of requests that can be sent on a persistent connection to the service. Note: Connection requests beyond this value are rejected. Minimum value = 0 Maximum value = 65535
cacheable	<String>	Read-write	Use the transparent cache redirection virtual server to forward requests to the cache server. Note: Do not specify this parameter if you set the Cache Type parameter. Default value: NO Possible values = YES, NO
cip	<String>	Read-write	Before forwarding a request to the service, insert an HTTP header with the client's IPv4 or IPv6 address as its value. Used if the server needs the client's IP address for security,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			accounting, or other purposes, and setting the Use Source IP parameter is not a viable option. Possible values = ENABLED, DISABLED
cipheader	<String>	Read-write	Name for the HTTP header whose value must be set to the IP address of the client. Used with the Client IP parameter. If you set the Client IP parameter, and you do not specify a name for the header, the appliance uses the header name specified for the global Client IP Header parameter (the cipHeader parameter in the set ns param CLI command or the Client IP Header parameter in the Configure HTTP Parameters dialog box at System > Settings > Change HTTP parameters). If the global Client IP Header parameter is not specified, the appliance inserts a

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			header with the name "client-ip.". Minimum length = 1
usip	<String>	Read-write	Use the client's IP address as the source IP address when initiating a connection to the server. When creating a service, if you do not set this parameter, the service inherits the global Use Source IP setting (available in the enable ns mode and disable ns mode CLI commands, or in the System > Settings > Configure modes > Configure Modes dialog box). However, you can override this setting after you create the service. Possible values = YES, NO
pathmonitor	<String>	Read-write	Path monitoring for clustering. Possible values = YES, NO
pathmonitorindv	<String>	Read-write	Individual Path monitoring decisions. Possible values = YES, NO

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
useproxyport	<String>	Read-write	Use the proxy port as the source port when initiating connections with the server. With the NO setting, the client-side connection port is used as the source port for the server-side connection. Note: This parameter is available only when the Use Source IP (USIP) parameter is set to YES. Possible values = YES, NO
sp	<String>	Read-write	Enable surge protection for the service. Possible values = ON, OFF
rtspsessionidremap	<String>	Read-write	Enable RTSP session ID mapping for the service. Default value: OFF Possible values = ON, OFF
clttimeout	<Integer>	Read-write	Time, in seconds, after which to terminate an idle client connection.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum value = 0 Maximum value = 31536000
svrtimeout	<Integer>	Read-write	Time, in seconds, after which to terminate an idle server connection. Minimum value = 0 Maximum value = 31536000
customserverid	<String>	Read-write	Unique identifier for the service. Used when the persistency type for the virtual server is set to Custom Server ID. Default value: "None"
serverid	<Integer>	Read-write	The identifier for the service. This is used when the persistency type is set to Custom Server ID.
cka	<String>	Read-write	Enable client keep-alive for the service. Possible values = YES, NO
tcpb	<String>	Read-write	Enable TCP buffering for the service. Possible values = YES, NO

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
cmp	<String>	Read-write	Enable compression for the service. Possible values = YES, NO
maxbandwidth	<Integer>	Read-write	Maximum bandwidth, in Kbps, allocated to the service. Minimum value = 0 Maximum value = 4294967287
accessdown	<String>	Read-write	Use Layer 2 mode to bridge the packets sent to this service if it is marked as DOWN. If the service is DOWN, and this parameter is disabled, the packets are dropped. Default value: NO Possible values = YES, NO
monthreshold	<Integer>	Read-write	Minimum sum of weights of the monitors that are bound to this service. Used to determine whether to mark a service as UP or DOWN. Minimum value = 0 Maximum value = 65535

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
state	<String>	Read-write	Initial state of the service. Default value: ENABLED Possible values = ENABLED, DISABLED
downstateflush	<String>	Read-write	Flush all active transactions associated with a service whose state transitions from UP to DOWN. Do not enable this option for applications that must complete their transactions. Default value: ENABLED Possible values = ENABLED, DISABLED
tcpprofilename	<String>	Read-write	Name of the TCP profile that contains TCP configuration settings for the service. Minimum length = 1 Maximum length = 127
httpprofilename	<String>	Read-write	Name of the HTTP profile that contains HTTP configuration

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			settings for the service. Minimum length = 1 Maximum length = 127
contentinspectionprofilename	<String>	Read-write	Name of the ContentInspection profile that contains IPS/IDS communication related setting for the service. Minimum length = 1 Maximum length = 127
aigwprofilename	<String>	Read-write	Name of the AIGW Profile that contains AIGW Endpoint setting for the service. Minimum length = 1 Maximum length = 255
quicprofilename	<String>	Read-write	Name of QUIC profile which will be attached to the service. Minimum length = 1 Maximum length = 255
hashid	<Integer>	Read-write	A numerical identifier that can be used by hash based load

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			balancing methods. Must be unique for each service. Minimum value = 1
comment	<String>	Read-write	Any information about the service.
appflowlog	<String>	Read-write	Enable logging of AppFlow information. Default value: ENABLED Possible values = ENABLED, DISABLED
netprofile	<String>	Read-write	Network profile to use for the service. Minimum length = 1 Maximum length = 127
td	<Integer>	Read-write	Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0. Minimum value = 0 Maximum value = 4094

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
processlocal	<String>	Read-write	By turning on this option packets destined to a service in a cluster will not under go any steering. Turn this option for single packet request response mode or when the upstream device is performing a proper RSS for connection based distribution. Default value: DISABLED Possible values = ENABLED, DISABLED
dnsprofilename	<String>	Read-write	Name of the DNS profile to be associated with the service. DNS profile properties will applied to the transactions processed by a service. This parameter is valid only for ADNS, ADNS-TCP and ADNS-DOT services. Minimum length = 1 Maximum length = 127

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
monconnectionclose	<String>	Read-write	Close monitoring connections by sending the service a connection termination message with the specified bit set. Default value: NONE Possible values = RESET, FIN
mcpprofilename	<String>	Read-write	Name of MCP profile which will be attached to the service.
ipaddress	<String>	Read-write	The new IP address of the service.
weight	<Integer>	Read-write	Weight to assign to the monitor-service binding. When a monitor is UP, the weight assigned to its binding with the service determines how much the monitor contributes toward keeping the health of the service above the value configured for the Monitor Threshold parameter. Minimum value = 1 Maximum value = 100

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
monitor_name_svc	<String>	Read-write	Name of the monitor bound to the specified service. Minimum length = 1
delay	<Integer>	Read-write	Time, in seconds, allocated to the NetScaler for a graceful shutdown of the service. During this period, new requests are sent to the service only for clients who already have persistent sessions on the appliance. Requests from new clients are load balanced among other available services. After the delay time expires, no requests are sent to the service, and the service is marked as unavailable (OUT OF SERVICE).
graceful	<String>	Read-write	Shut down gracefully, not accepting any new connections, and disabling the service when all of its connections are closed. Default value: NO

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = YES, NO
all	<Boolean>	Read-write	Display both user-configured and dynamically learned services.
Internal	<Boolean>	Read-write	Display only dynamically learned services.
newname	<String>	Read-write	New name for the service. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Minimum length = 1
numofconnections	<Integer>	Read-only	This will tell the number of client side connections are still open.
policyname	<String>	Read-only	The name of the policyname for which this service is bound.
serviceconftype	<Boolean>	Read-only	The configuration type of the service.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
serviceconftype2	<String>	Read-only	The configuration type of the service (Internal/Dynamic/ Configured). Possible values = Configured, Dynamic, Internal
value	<String>	Read-only	SSL status. Possible values = Certkey/ Certkeybundle/Vault not bound/Cert-store not usable, SSL feature disabled
gslb	<String>	Read-only	The GSLB option for the corresponding virtual server. Possible values = REMOTE, LOCAL
dup_state	<String>	Read-only	Added this field for getting state value from table. Possible values = ENABLED, DISABLED
publicip	<String>	Read-only	public ip.
publicport	<Integer>	Read-only	public port. Minimum value = 1 Range 1 - 65535 * in CLI is represented as

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			65535 in NITRO API
svrstate	<String>	Read-only	The state of the service. Possible values = UP, DOWN, UNKNOWN, BUSY, OUT OF SERVICE, GOING OUT OF SERVICE, DOWN WHEN GOING OUT OF SERVICE, NS_EMPTY_STR, Unknown, DISABLED
monitor_state	<String>	Read-only	The running state of the monitor on this service. Possible values = UP, DOWN, UNKNOWN, BUSY, OUT OF SERVICE, GOING OUT OF SERVICE, DOWN WHEN GOING OUT OF SERVICE, NS_EMPTY_STR, Unknown, DISABLED
monstatcode	<Integer>	Read-only	The code indicating the monitor response.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
lastresponse	<String>	Read-only	The string form of monstatcode.
responsetime	<Integer>	Read-only	Response time of this monitor.
monstatparam1	<Integer>	Read-only	First parameter for use with message code.
monstatparam2	<Integer>	Read-only	Second parameter for use with message code.
monstatparam3	<Integer>	Read-only	Third parameter for use with message code.
statechangetimesec	<String>	Read-only	Time when last state change happened. Seconds part.
statechangetimemsec	<Integer>	Read-only	Time at which last state change happened. Milliseconds part.
tickssincelaststatechange	<Integer>	Read-only	Time in 10 millisecond ticks since the last state change.
stateupdatereason	<Integer>	Read-only	Checks state update reason on the secondary node.
clmonowner	<Integer>	Read-only	Tells the mon owner of the service. Minimum value = 0

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum value = 32
clmonview	<Integer>	Read-only	Tells the view id of the monitoring owner.
serviceipstr	<String>	Read-only	This field has been intorduced to show the dbs services ip.
oracleserverversion	<String>	Read-only	Oracle server version. Default value: 10G Possible values = 10G, 11G
nodefaultbindings	<String>	Read-only	to determine if the configuration will have default ssl CIPHER and ECC curve bindings. Default value: NO Possible values = YES, NO
monuserstatusmesg	<String>	Read-only	This field has been introduced to show user monitor failure reasons.
builtin	<String[]>	Read-only	. Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
feature	<String>	Read-only	The feature to be checked while applying this config.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- ENABLE
- DISABLE
- GET (ALL)
- GET
- COUNT
- RENAME

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of

creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/service **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"service":{

<b>"name":<String_value>,

</b>"ip":<String_value>,

"servername":<String_value>,

<b>"servicetype":<String_value>,

</b><b>"port":<Integer_value>,

</b>"cleartextport":<Integer_value>,

"cachetype":<String_value>,

"maxclient":<Integer_value>,
```

```
"healthmonitor":<String_value>,

"maxreq":<Integer_value>,

"cacheable":<String_value>,

"cip":<String_value>,

"cipheader":<String_value>,

"usip":<String_value>,

"pathmonitor":<String_value>,

"pathmonitorindv":<String_value>,

"useproxyport":<String_value>,

"sp":<String_value>,

"rtspsessionidremap":<String_value>,

"clttimeout":<Integer_value>,

"svrtimeout":<Integer_value>,

"customserverid":<String_value>,

"serverid":<Integer_value>,

"cka":<String_value>,

"tcpb":<String_value>,

"cmp":<String_value>,

"maxbandwidth":<Integer_value>,

"accessdown":<String_value>,

"monthreshold":<Integer_value>,

"state":<String_value>,
```

```
"downstateflush":<String_value>,

"tcpprofilename":<String_value>,

"httpprofilename":<String_value>,

"contentinspectionprofilename":<String_value>,

"aigwprofilename":<String_value>,

"quicprofilename":<String_value>,

"hashid":<Integer_value>,

"comment":<String_value>,

"appflowlog":<String_value>,

"netprofile":<String_value>,

"td":<Integer_value>,

"processlocal":<String_value>,

"dnsprofilename":<String_value>,

"monconnectionclose":<String_value>,

"mcpprofilename":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/service/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/service **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"service":{

<b>"name":<String_value>,

</b>"ipaddress":<String_value>,

"maxclient":<Integer_value>,

"maxreq":<Integer_value>,

"cacheable":<String_value>,

"cip":<String_value>,

"cipheader":<String_value>,

"usip":<String_value>,

"pathmonitor":<String_value>,

"pathmonitorindv":<String_value>,

"useproxyport":<String_value>,
```

```
"sp":<String_value>,

"rtspsessionidremap":<String_value>,

"healthmonitor":<String_value>,

"clttimeout":<Integer_value>,

"svrtimeout":<Integer_value>,

"customserverid":<String_value>,

"serverid":<Integer_value>,

"cka":<String_value>,

"tcpb":<String_value>,

"cmp":<String_value>,

"maxbandwidth":<Integer_value>,

"accessdown":<String_value>,

"monthreshold":<Integer_value>,

"weight":<Integer_value>,

"monitor_name_svc":<String_value>,

"downstateflush":<String_value>,

"tcpprofilename":<String_value>,

"httpprofilename":<String_value>,

"contentinspectionprofilename":<String_value>,

"quicprofilename":<String_value>,

"hashid":<Integer_value>,

"comment":<String_value>,
```

```
"appflowlog":<String_value>,

"netprofile":<String_value>,

"processlocal":<String_value>,

"dnsprofilename":<String_value>,

"monconnectionclose":<String_value>,

"mcpprofilename":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/service? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"service":{

<b>"name":<String_value>,

</b>"maxclient":true,

"maxreq":true,

"cacheable":true,

"cip":true,
```

```
"usip":true,

"pathmonitor":true,

"pathmonitorindv":true,

"useproxyport":true,

"sp":true,

"rtspsessionidremap":true,

"customserverid":true,

"serverid":true,

"cka":true,

"tcpb":true,

"cmp":true,

"maxbandwidth":true,

"accessdown":true,

"monthreshold":true,

"clttimeout":true,

"svrtimeout":true,

"tcpprofilename":true,

"httpprofilename":true,

"contentinspectionprofilename":true,

"hashid":true,

"appflowlog":true,

"netprofile":true,
```

```
"processlocal":true,

"dnsprofilename":true,

"quicprofilename":true,

"monconnectionclose":true,

"cipheader":true,

"healthmonitor":true,

"downstateflush":true,

"comment":true,

"mcpprofilename":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

ENABLE

URL: http:// <netscaler-ip-address> /nitro/v1/config/service? **action=enable HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"service":{

<b>"name":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DISABLE

URL: http:// <netscaler-ip-address> /nitro/v1/config/service? **action=disable HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"service":{

<b>"name":<String_value>,

</b>"delay":<Integer_value>,

"graceful":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

RENAME

URL: http:// <netscaler-ip-address> /nitro/v1/config/service? **action=rename HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"service":{

<b>"name":<String_value>,

</b><b>"newname":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/service **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/service? **args=name: <String_value> ,all: <Boolean_value> ,Internal: <Boolean_value>**

Use this query-parameter to get service resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/config/service? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/service? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of service resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/service? **view=summary**

Use this query-parameter to get the summary output of service resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/service? **pagesize=#no;pageno=#no**

Use this query-parameter to get the service resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "service": [ {

name:<String_value>,all:<Boolean_value>,Internal:<Boolean_value>"numofconn
ections":<Integer_value>,

"servername":<String_value>,

"policyname":<String_value>,

"servicetype":<String_value>,

"serviceconftpye":<Boolean_value>,

"serviceconftype":<Boolean_value>,

"serviceconftype2":<String_value>,

"port":<Integer_value>,

"value":<String_value>,

"cleartextport":<Integer_value>,

"gslb":<String_value>,
```

```
"cachetype":<String_value>,

"maxclient":<Integer_value>,

"maxreq":<Integer_value>,

"cacheable":<String_value>,

"cip":<String_value>,

"cipheader":<String_value>,

"usip":<String_value>,

"pathmonitor":<String_value>,

"pathmonitorindv":<String_value>,

"useproxyport":<String_value>,

"dup_state":<String_value>,

"sp":<String_value>,

"rtspsessionidremap":<String_value>,

"clttimeout":<Integer_value>,

"svrtimeout":<Integer_value>,

"publicip":<String_value>,

"publicport":<Integer_value>,

"customserverid":<String_value>,

"serverid":<Integer_value>,

"cka":<String_value>,

"tcpb":<String_value>,

"processlocal":<String_value>,
```

```
"cmp":<String_value>,

"maxbandwidth":<Integer_value>,

"accessdown":<String_value>,

"svrstate":<String_value>,

"delay":<Integer_value>,

"ipaddress":<String_value>,

"monthreshold":<Integer_value>,

"monitor_state":<String_value>,

"monstatcode":<Integer_value>,

"lastresponse":<String_value>,

"responsetime":<Integer_value>,

"monstatparam1":<Integer_value>,

"monstatparam2":<Integer_value>,

"monstatparam3":<Integer_value>,

"downstateflush":<String_value>,

"statechangetimesec":<String_value>,

"statechangetimemsec":<Integer_value>,

"timesincelaststatechange":<Integer_value>,

"tickssincelaststatechange":<Integer_value>,

"stateupdatereason":<Integer_value>,

"clmonowner":<Integer_value>,

"clmonview":<Integer_value>,
```

```
"tcpprofilename":<String_value>,

"httpprofilename":<String_value>,

"contentinspectionprofilename":<String_value>,

"aigwprofilename":<String_value>,

"quicprofilename":<String_value>,

"hashid":<Integer_value>,

"graceful":<String_value>,

"comment":<String_value>,

"healthmonitor":<String_value>,

"appflowlog":<String_value>,

"netprofile":<String_value>,

"serviceipstr":<String_value>,

"weight":<Integer_value>,

"td":<Integer_value>,

"oracleserverversion":<String_value>,

"dnsprofilename":<String_value>,

"monconnectionclose":<String_value>,

"nodefaultbindings":<String_value>,

"monuserstatusmesg":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"mcpprofilename":<String_value>,
```

```
"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/service/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/service/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/service/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of service resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "service": [ {

name:<String_value>,all:<Boolean_value>,Internal:<Boolean_value>"numofconn
ections":<Integer_value>,

"servername":<String_value>,
```

```
"policyname":<String_value>,

"servicetype":<String_value>,

"serviceconftpye":<Boolean_value>,

"serviceconftype":<Boolean_value>,

"serviceconftype2":<String_value>,

"port":<Integer_value>,

"value":<String_value>,

"cleartextport":<Integer_value>,

"gslb":<String_value>,

"cachetype":<String_value>,

"maxclient":<Integer_value>,

"maxreq":<Integer_value>,

"cacheable":<String_value>,

"cip":<String_value>,

"cipheader":<String_value>,

"usip":<String_value>,

"pathmonitor":<String_value>,

"pathmonitorindv":<String_value>,

"useproxyport":<String_value>,

"dup_state":<String_value>,

"sp":<String_value>,

"rtspsessionidremap":<String_value>,
```

```
"clttimeout":<Integer_value>,

"svrtimeout":<Integer_value>,

"publicip":<String_value>,

"publicport":<Integer_value>,

"customserverid":<String_value>,

"serverid":<Integer_value>,

"cka":<String_value>,

"tcpb":<String_value>,

"processlocal":<String_value>,

"cmp":<String_value>,

"maxbandwidth":<Integer_value>,

"accessdown":<String_value>,

"svrstate":<String_value>,

"delay":<Integer_value>,

"ipaddress":<String_value>,

"monthreshold":<Integer_value>,

"monitor_state":<String_value>,

"monstatcode":<Integer_value>,

"lastresponse":<String_value>,

"responsetime":<Integer_value>,

"monstatparam1":<Integer_value>,

"monstatparam2":<Integer_value>,
```

```
"monstatparam3":<Integer_value>,

"downstateflush":<String_value>,

"statechangetimesec":<String_value>,

"statechangetimemsec":<Integer_value>,

"timesincelaststatechange":<Integer_value>,

"tickssincelaststatechange":<Integer_value>,

"stateupdatereason":<Integer_value>,

"clmonowner":<Integer_value>,

"clmonview":<Integer_value>,

"tcpprofilename":<String_value>,

"httpprofilename":<String_value>,

"contentinspectionprofilename":<String_value>,

"aigwprofilename":<String_value>,

"quicprofilename":<String_value>,

"hashid":<Integer_value>,

"graceful":<String_value>,

"comment":<String_value>,

"healthmonitor":<String_value>,

"appflowlog":<String_value>,

"netprofile":<String_value>,

"serviceipstr":<String_value>,

"weight":<Integer_value>,
```

```
"td":<Integer_value>,

"oracleserverversion":<String_value>,

"dnsprofilename":<String_value>,

"monconnectionclose":<String_value>,

"nodefaultbindings":<String_value>,

"monuserstatusmesg":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"mcpprofilename":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/service? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "service": [ { "__count": "#no"} ] }
```

service_binding

Binding object which returns the resources bound to service.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the service for which to display configuration details. Minimum length = 1
service_lbmonitor_binding	<service_lbmonitor_binding[]>	Read-only	lbmonitor that can be bound to service.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/service_binding/ name_value<String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "service_binding": [ {

"name":<String_value>,

"service_lbmonitor_binding":<service_lbmonitor_binding[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/service_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/service_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "service_binding": [ {

"name":<String_value>,

"service_lbmonitor_binding":<service_lbmonitor_binding[]_value>

}]}
```

service_lbmonitor_binding

Binding object showing the lbmonitor that can be bound to service.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
monstate	<String>	Read-write	The configured state (enable/disable) of the monitor on this server. Possible values = ENABLED, DISABLED
weight	<Integer>	Read-write	Weight to assign to the monitor-service binding. When a monitor is UP, the weight assigned to its binding with the service determines how much the monitor contributes toward keeping the health of the service above the value configured for the Monitor Threshold parameter. Minimum value = 1 Maximum value = 100
name	<String>	Read-write	Name of the service to which to bind a monitor. Minimum length = 1
passive	<Boolean>	Read-write	Indicates if load monitor is passive. A passive load monitor does not remove service from LB decision when

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			threshold is breached.
monitor_name	<String>	Read-write	The monitor Names.
monitorcurrentfailedprobes	<Integer>	Read-only	Total number of currently failed probes.
dup_state	<String>	Read-only	Added this field for getting state value from table. Possible values = ENABLED, DISABLED
dup_weight	<Integer>	Read-only	The weight of the monitor.
totalprobes	<Integer>	Read-only	The total number of probs sent.
monitortotalprobes	<Integer>	Read-only	Total number of probes sent to monitor this service.
monstatcode	<Integer>	Read-only	The code indicating the monitor response.
monitor_state	<String>	Read-only	The running state of the monitor on this service. Possible values = UP, DOWN, UNKNOWN, BUSY, OUT OF SERVICE, GOING OUT OF SERVICE, DOWN WHEN GOING

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			OUT OF SERVICE, NS_EMPTY_STR, Unknown, DISABLED
monstatparam1	<Integer>	Read-only	First parameter for use with message code.
lastresponse	<String>	Read-only	The string form of monstatcode.
responsetime	<Integer>	Read-only	Response time of this monitor.
monstatparam3	<Integer>	Read-only	Third parameter for use with message code.
failedprobes	<Integer>	Read-only	Number of the current failed monitoring probes.
totalfailedprobes	<Integer>	Read-only	The total number of failed probs.
monstatparam2	<Integer>	Read-only	Second parameter for use with message code.
monitortotalfailedprobes	<Integer>	Read-only	Total number of failed probes.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/service_lbmonitor_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"service_lbmonitor_binding":{

<b>"name":<String_value>,

</b>"monitor_name":<String_value>,

"monstate":<String_value>,

"weight":<Integer_value>,

"passive":<Boolean_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/service_lbmonitor_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ service_lbmonitor_binding/ name_value<String> ? **args=monitor_name: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/service_lbmonitor_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/

service_lbmonitor_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of service_lbmonitor_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/service_lbmonitor_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the service_lbmonitor_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "service_lbmonitor_binding": [ {

"monstate":<String_value>,

"weight":<Integer_value>,

"name":<String_value>,

"passive":<Boolean_value>,

"monitor_name":<String_value>,

"monitorcurrentfailedprobes":<Integer_value>,
```

```
"dup_state":<String_value>,

"dup_weight":<Integer_value>,

"totalprobes":<Integer_value>,

"monitortotalprobes":<Integer_value>,

"monstatcode":<Integer_value>,

"monitor_state":<String_value>,

"monstatparam1":<Integer_value>,

"lastresponse":<String_value>,

"responsetime":<Integer_value>,

"monstatparam3":<Integer_value>,

"failedprobes":<Integer_value>,

"totalfailedprobes":<Integer_value>,

"monstatparam2":<Integer_value>,

"monitortotalfailedprobes":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/service_lbmonitor_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/service_lbmonitor_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "service_lbmonitor_binding": [ {

"monstate":<String_value>,

"weight":<Integer_value>,

"name":<String_value>,

"passive":<Boolean_value>,

"monitor_name":<String_value>,

"monitorcurrentfailedprobes":<Integer_value>,

"dup_state":<String_value>,

"dup_weight":<Integer_value>,

"totalprobes":<Integer_value>,

"monitortotalprobes":<Integer_value>,

"monstatcode":<Integer_value>,

"monitor_state":<String_value>,

"monstatparam1":<Integer_value>,

"lastresponse":<String_value>,
```

```
"responsetime":<Integer_value>,

"monstatparam3":<Integer_value>,

"failedprobes":<Integer_value>,

"totalfailedprobes":<Integer_value>,

"monstatparam2":<Integer_value>,

"monitortotalfailedprobes":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/service_lbmonitor_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"service_lbmonitor_binding": [ { "__count": "#no"} ] }
```

servicegroup

Configuration for service group resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
servicegroupname	<String>	Read-write	Name of the service group. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Can be changed after the name is created. Minimum length = 1
servicetype	<String>	Read-write	Protocol used to exchange data with the service. Possible values = HTTP, FTP, TCP, UDP, SSL, SSL_BRIDGE, SSL_TCP, DTLS, NNTP, RPCSVR, DNS, ADNS, SNMP, RTSP, DHCPRA, ANY, SIP_UDP, SIP_TCP, SIP_SSL, DNS_TCP, ADNS_TCP, MYSQL, MSSQL, ORACLE, MONGO,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			MONGO_TLS, RADIUS, RADIUSListener, RDP, DIAMETER, SSL_DIAMETER, TFTP, SMPP, PPTP, GRE, SYSLOGTCP, SYSLOGUDP, FIX, SSL_FIX, USER_TCP, USER_SSL_TCP, QUIC, IPFIX, LOGSTREAM, LOGSTREAM_SSL, MQTT, MQTT_TLS, QUIC_BRIDGE, DOT, ADNS_DOT, HTTP_QUIC, ADNS_DOH, KAFKA_BROKER
cachetype	<String>	Read-write	Cache type supported by the cache server. Possible values = TRANSPARENT, REVERSE, FORWARD
td	<Integer>	Read-write	Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			domain, which has an ID of 0. Minimum value = 0 Maximum value = 4094
maxclient	<Integer>	Read-write	Maximum number of simultaneous open connections for the service group. Minimum value = 0 Maximum value = 4294967294
maxreq	<Integer>	Read-write	Maximum number of requests that can be sent on a persistent connection to the service group. Note: Connection requests beyond this value are rejected. Minimum value = 0 Maximum value = 65535
cacheable	<String>	Read-write	Use the transparent cache redirection virtual server to forward the request to the cache server. Note: Do not set this parameter if

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			you set the Cache Type. Default value: NO Possible values = YES, NO
cip	<String>	Read-write	Insert the Client IP header in requests forwarded to the service. Possible values = ENABLED, DISABLED
cipheader	<String>	Read-write	Name of the HTTP header whose value must be set to the IP address of the client. Used with the Client IP parameter. If client IP insertion is enabled, and the client IP header is not specified, the value of Client IP Header parameter or the value set by the set ns config command is used as client's IP header name. Minimum length = 1
usip	<String>	Read-write	Use client's IP address as the source IP address when initiating connection to the server. With the NO

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			setting, which is the default, a mapped IP (MIP) address or subnet IP (SNIP) address is used as the source IP address to initiate server side connections. Possible values = YES, NO
pathmonitor	<String>	Read-write	Path monitoring for clustering. Possible values = YES, NO
pathmonitorindv	<String>	Read-write	Individual Path monitoring decisions. Possible values = YES, NO
useproxyport	<String>	Read-write	Use the proxy port as the source port when initiating connections with the server. With the NO setting, the client-side connection port is used as the source port for the server-side connection. Note: This parameter is available only when the Use Source IP (USIP) parameter is set to YES.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = YES, NO
healthmonitor	<String>	Read-write	Monitor the health of this service. Available settings function as follows: YES - Send probes to check the health of the service. NO - Do not send probes to check the health of the service. With the NO option, the appliance shows the service as UP at all times. Default value: YES Possible values = YES, NO
sp	<String>	Read-write	Enable surge protection for the service group. Default value: OFF Possible values = ON, OFF
rtspsessionidremap	<String>	Read-write	Enable RTSP session ID mapping for the service group. Default value: OFF

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ON, OFF
clttimeout	<Integer>	Read-write	Time, in seconds, after which to terminate an idle client connection. Minimum value = 0 Maximum value = 31536000
svrtimeout	<Integer>	Read-write	Time, in seconds, after which to terminate an idle server connection. Minimum value = 0 Maximum value = 31536000
cka	<String>	Read-write	Enable client keep-alive for the service group. Possible values = YES, NO
tcpb	<String>	Read-write	Enable TCP buffering for the service group. Possible values = YES, NO
cmp	<String>	Read-write	Enable compression for the specified service. Possible values = YES, NO

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
maxbandwidth	<Integer>	Read-write	Maximum bandwidth, in Kbps, allocated for all the services in the service group. Minimum value = 0 Maximum value = 4294967287
monthreshold	<Integer>	Read-write	Minimum sum of weights of the monitors that are bound to this service. Used to determine whether to mark a service as UP or DOWN. Minimum value = 0 Maximum value = 65535
state	<String>	Read-write	Initial state of the service group. Default value: ENABLED Possible values = ENABLED, DISABLED
downstateflush	<String>	Read-write	Flush all active transactions associated with all the services in the service group whose state transitions from UP to DOWN. Do not enable this option for applications that

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			must complete their transactions. Default value: ENABLED Possible values = ENABLED, DISABLED
tcpprofilename	<String>	Read-write	Name of the TCP profile that contains TCP configuration settings for the service group. Minimum length = 1 Maximum length = 127
httpprofilename	<String>	Read-write	Name of the HTTP profile that contains HTTP configuration settings for the service group. Minimum length = 1 Maximum length = 127
aigwprofilename	<String>	Read-write	Name of the backend AIGW Profile which will be attached to the servicegroup. This parameter enables the servicegroup to process the LLM request/response based on the profile config. Any service item bound to the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			servicegroup will inherit the backend AIGW Profile bound at the servicegroup level, if it does not have an explicit AIGW Profile given at bind time. Minimum length = 1 Maximum length = 255
quicprofilename	<String>	Read-write	Name of QUIC profile which will be attached to the service group. Minimum length = 1 Maximum length = 255
comment	<String>	Read-write	Any information about the service group.
appflowlog	<String>	Read-write	Enable logging of AppFlow information for the specified service group. Default value: ENABLED Possible values = ENABLED, DISABLED
netprofile	<String>	Read-write	Network profile for the service group. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum length = 127
autoscale	<String>	Read-write	Auto scale option for a servicegroup. Default value: DISABLED Possible values = DISABLED, DNS, POLICY, CLOUD, API
memberport	<Integer>	Read-write	member port.
autodisablegraceful	<String>	Read-write	Indicates graceful shutdown of the service. System will wait for all outstanding connections to this service to be closed before disabling the service. Default value: NO Possible values = YES, NO
autodisabledelay	<Integer>	Read-write	The time allowed (in seconds) for a graceful shutdown. During this period, new connections or requests will continue to be sent to this service for clients who already have a persistent session on the system. Connections

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			or requests from fresh or new clients who do not yet have a persistence sessions on the system will not be sent to the service. Instead, they will be load balanced among other available services. After the delay time expires, no new requests or connections will be sent to the service.
autodelayedtrofs	<String>	Read-write	Indicates graceful movement of IP-Port binding/s to TROFS when IP addresses are removed from DNS response. System will wait for monitor response timeout period before moving to TROFS . Default value: NO Possible values = YES, NO
monconnectionclose	<String>	Read-write	Close monitoring connections by sending the service a connection termination message with the specified bit set.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: NONE Possible values = RESET, FIN
bootstrap	<String>	Read-write	Flag to check if kafka broker servicegroup is of type bootstrap or not. Default value: NO Possible values = YES, NO
topicname	<String>	Read-write	Name of the Kafka topic.
mcpprofilename	<String>	Read-write	Name of MCP profile which will be attached to the servicegroup.
servername	<String>	Read-write	Name of the server to which to bind the service group. Minimum length = 1
port	<Integer>	Read-write	Server port number. Range 1 - 65535 * in CLI is represented as 65535 in NITRO API
weight	<Integer>	Read-write	Weight to assign to the servers in the service group. Specifies the capacity of the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			servers relative to the other servers in the load balancing configuration. The higher the weight, the higher the percentage of requests sent to the service. Minimum value = 1 Maximum value = 100
customserverid	<String>	Read-write	The identifier for this IP:Port pair. Used when the persistency type is set to Custom Server ID. Default value: "None"
serverid	<Integer>	Read-write	The identifier for the service. This is used when the persistency type is set to Custom Server ID.
hashid	<Integer>	Read-write	The hash identifier for the service. This must be unique for each service. This parameter is used by hash based load balancing methods. Minimum value = 1
nameserver	<String>	Read-write	Specify the nameserver to which the query for bound domain needs to be

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			sent. If not specified, use the global nameserver.
dbsttl	<Integer>	Read-write	Specify the TTL for DNS record for domain based service.The default value of ttl is 0 which indicates to use the TTL received in DNS response for monitors. Default value: 0
order	<Integer>	Read-write	Order number to be assigned to the servicegroup member. Minimum value = 1 Maximum value = 8192
monitor_name_svc	<String>	Read-write	Name of the monitor bound to the service group. Used to assign a weight to the monitor. Minimum length = 1
dup_weight	<Integer>	Read-write	weight of the monitor that is bound to servicegroup. Minimum value = 1
delay	<Integer>	Read-write	Time, in seconds, allocated for a shutdown of the services in the service group.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			During this period, new requests are sent to the service only for clients who already have persistent sessions on the appliance. Requests from new clients are load balanced among other available services. After the delay time expires, no requests are sent to the service, and the service is marked as unavailable (OUT OF SERVICE).
graceful	<String>	Read-write	Wait for all existing connections to the service to terminate before shutting down the service. Default value: NO Possible values = YES, NO
includemembers	<Boolean>	Read-write	Display the members of the listed service groups in addition to their settings. Can be specified when no service group name is provided in the command. In that case, the details displayed for each service group are identical to the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			details displayed when a service group name is provided, except that bound monitors are not displayed.
newname	<String>	Read-write	New name for the service group. Minimum length = 1
numofconnections	<Integer>	Read-only	This will tell the number of client side connections are still open.
serviceconftype	<Boolean>	Read-only	The configuration type of the service group.
value	<String>	Read-only	SSL Status. Possible values = Certkey/ Certkeybundle/Vault not bound/Cert-store not usable, SSL feature disabled
svrstate	<String>	Read-only	The state of the service. Possible values = UP, DOWN, UNKNOWN, BUSY, OUT OF SERVICE, GOING OUT OF SERVICE, DOWN WHEN GOING OUT OF SERVICE,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			NS_EMPTY_STR, Unknown, DISABLED
ip	<String>	Read-only	IP Address.
monstatcode	<Integer>	Read-only	The code indicating the monitor response.
monstatparam1	<Integer>	Read-only	First parameter for use with message code.
monstatparam2	<Integer>	Read-only	Second parameter for use with message code.
monstatparam3	<Integer>	Read-only	Third parameter for use with message code.
statechangetimemsec	<Integer>	Read-only	Time when last state change occurred. Milliseconds part.
stateupdatereason	<Integer>	Read-only	Checks state update reason on the secondary node.
clmonowner	<Integer>	Read-only	Tells the mon owner of the service.
clmonview	<Integer>	Read-only	Tells the view id of the monitoring owner.
groupcount	<Integer>	Read-only	Servicegroup Count.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
serviceipstr	<String>	Read-only	This field has been intorduced to show the dbs services ip.
servicegroupeffective state	<String>	Read-only	Indicates the effective servicegroup state based on the state of the bound service items.If all services are UP the effective state is UP, if all are DOWN its DOWN,if all are OFS its OFS.If atleast one serviceis UP and rest are either DOWN or OFS, the effective state is PARTIAL-UP.If atleast one bound service is DOWN and rest are OFS the effective state is PARTIAL DOWN. Possible values = UP, DOWN, OUT OF SERVICE, PARTIAL-UP, PARTIAL-DOWN
nodefaultbindings	<String>	Read-only	to determine if the configuration is from stylebooks. Default value: NO Possible values = YES, NO

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
svcitmactsvcs	<Integer>	Read-only	This gives the total active service items for an FQDN for SRV type server binding.
svcitmboundsvcs	<Integer>	Read-only	This gives the total bound items for an FQDN for SRV type server binding.
monuserstatusmesg	<String>	Read-only	This field has been introduced to show user monitor failure reasons.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- ENABLE
- DISABLE
- GET (ALL)
- GET
- COUNT
- RENAME

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/servicegroup **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"servicegroup":{

<b>"servicegroupname":<String_value>,

</b><b>"servicetype":<String_value>,

</b>"cachetype":<String_value>,
```

```
"td":<Integer_value>,

"maxclient":<Integer_value>,

"maxreq":<Integer_value>,

"cacheable":<String_value>,

"cip":<String_value>,

"cipheader":<String_value>,

"usip":<String_value>,

"pathmonitor":<String_value>,

"pathmonitorindv":<String_value>,

"useproxyport":<String_value>,

"healthmonitor":<String_value>,

"sp":<String_value>,

"rtspsessionidremap":<String_value>,

"clttimeout":<Integer_value>,

"svrtimeout":<Integer_value>,

"cka":<String_value>,

"tcpb":<String_value>,

"cmp":<String_value>,

"maxbandwidth":<Integer_value>,

"monthreshold":<Integer_value>,

"state":<String_value>,

"downstateflush":<String_value>,
```

```
"tcpprofilename":<String_value>,

"httpprofilename":<String_value>,

"aigwprofilename":<String_value>,

"quicprofilename":<String_value>,

"comment":<String_value>,

"appflowlog":<String_value>,

"netprofile":<String_value>,

"autoscale":<String_value>,

"memberport":<Integer_value>,

"autodisablegraceful":<String_value>,

"autodisabledelay":<Integer_value>,

"autodelayedtrofs":<String_value>,

"monconnectionclose":<String_value>,

"bootstrap":<String_value>,

"topicname":<String_value>,

"mcpprofilename":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/servicegroup/ servicegroupname_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/servicegroup **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"servicegroup":{

<b>"servicegroupname":<String_value>,

</b>"servername":<String_value>,

"port":<Integer_value>,

"weight":<Integer_value>,

"customserverid":<String_value>,

"serverid":<Integer_value>,

"hashid":<Integer_value>,

"nameserver":<String_value>,

"dbsttl":<Integer_value>,
```

```
"order":<Integer_value>,

"monitor_name_svc":<String_value>,

"dup_weight":<Integer_value>,

"maxclient":<Integer_value>,

"maxreq":<Integer_value>,

"healthmonitor":<String_value>,

"cacheable":<String_value>,

"cip":<String_value>,

"cipheader":<String_value>,

"usip":<String_value>,

"pathmonitor":<String_value>,

"pathmonitorindv":<String_value>,

"useproxyport":<String_value>,

"sp":<String_value>,

"rtspsessionidremap":<String_value>,

"clttimeout":<Integer_value>,

"svrtimeout":<Integer_value>,

"cka":<String_value>,

"tcpb":<String_value>,

"cmp":<String_value>,

"maxbandwidth":<Integer_value>,

"monthreshold":<Integer_value>,
```

```
"downstateflush":<String_value>,

"tcpprofilename":<String_value>,

"httpprofilename":<String_value>,

"quicprofilename":<String_value>,

"comment":<String_value>,

"appflowlog":<String_value>,

"netprofile":<String_value>,

"autodisablegraceful":<String_value>,

"autodisabledelay":<Integer_value>,

"autodelayedtrofs":<String_value>,

"monconnectionclose":<String_value>,

"autoscale":<String_value>,

"mcpprofilename":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/servicegroup? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"servicegroup":{

<b>"servicegroupname":<String_value>,

</b>"servername":true,

"port":true,

"weight":true,

"customserverid":true,

"serverid":true,

"hashid":true,

"nameserver":true,

"dbsttl":true,

"order":true,

"maxclient":true,

"maxreq":true,

"cacheable":true,

"cip":true,

"usip":true,

"useproxyport":true,

"sp":true,

"rtspsessionidremap":true,

"clttimeout":true,

"svrtimeout":true,
```

```
"cka":true,

"tcpb":true,

"cmp":true,

"maxbandwidth":true,

"monthreshold":true,

"tcpprofilename":true,

"httpprofilename":true,

"quicprofilename":true,

"appflowlog":true,

"netprofile":true,

"autodisablegraceful":true,

"autodisabledelay":true,

"monitor_name_svc":true,

"dup_weight":true,

"healthmonitor":true,

"cipheader":true,

"pathmonitor":true,

"pathmonitorindv":true,

"downstateflush":true,

"comment":true,

"autodelayedtrofs":true,

"monconnectionclose":true,
```

```
"mcpprofilename":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

ENABLE

URL: http:// <netscaler-ip-address> /nitro/v1/config/servicegroup? **action=enable HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"servicegroup":{

<b>"servicegroupname":<String_value>,

</b>"servername":<String_value>,

"port":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DISABLE

URL: http:// <netscaler-ip-address> /nitro/v1/config/servicegroup? **action=disable HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"servicegroup":{

<b>"servicegroupname":<String_value>,

</b>"servername":<String_value>,

"port":<Integer_value>,

"delay":<Integer_value>,

"graceful":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

RENAME

URL: http:// <netscaler-ip-address> /nitro/v1/config/servicegroup? **action=rename HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"servicegroup":{

<b>"servicegroupname":<String_value>,
```

```
</b><b>"newname":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/servicegroup **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/servicegroup? **args=servicegroupname: <String_value> ,includemembers: <Boolean_value>**

Use this query-parameter to get servicegroup resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/config/servicegroup? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/servicegroup? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of servicegroup resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/servicegroup? **view=summary**

Use this query-parameter to get the summary output of servicegroup resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/servicegroup? **pagesize=#no;pageno=#no**

Use this query-parameter to get the servicegroup resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "servicegroup": [ {

servicegroupname:<String_value>,includemembers:<Boolean_value>"numofconnec
tions":<Integer_value>,

"servicetype":<String_value>,

"port":<Integer_value>,

"td":<Integer_value>,

"serviceconftpye":<Boolean_value>,

"serviceconftype":<Boolean_value>,

"value":<String_value>,

"cachetype":<String_value>,

"maxclient":<Integer_value>,

"maxreq":<Integer_value>,

"cacheable":<String_value>,

"cip":<String_value>,

"cipheader":<String_value>,
```

```
"usip":<String_value>,

"pathmonitor":<String_value>,

"pathmonitorindv":<String_value>,

"useproxyport":<String_value>,

"sp":<String_value>,

"rtspsessionidremap":<String_value>,

"clttimeout":<Integer_value>,

"svrtimeout":<Integer_value>,

"cka":<String_value>,

"tcpb":<String_value>,

"cmp":<String_value>,

"maxbandwidth":<Integer_value>,

"state":<String_value>,

"svrstate":<String_value>,

"delay":<Integer_value>,

"ip":<String_value>,

"servername":<String_value>,

"monthreshold":<Integer_value>,

"weight":<Integer_value>,

"customserverid":<String_value>,

"serverid":<Integer_value>,

"monstatcode":<Integer_value>,
```

```
"monstatparam1":<Integer_value>,

"monstatparam2":<Integer_value>,

"monstatparam3":<Integer_value>,

"downstateflush":<String_value>,

"statechangetimemsec":<Integer_value>,

"timesincelaststatechange":<Integer_value>,

"stateupdatereason":<Integer_value>,

"clmonowner":<Integer_value>,

"clmonview":<Integer_value>,

"groupcount":<Integer_value>,

"comment":<String_value>,

"tcpprofilename":<String_value>,

"httpprofilename":<String_value>,

"aigwprofilename":<String_value>,

"quicprofilename":<String_value>,

"hashid":<Integer_value>,

"graceful":<String_value>,

"healthmonitor":<String_value>,

"appflowlog":<String_value>,

"netprofile":<String_value>,

"autoscale":<String_value>,

"memberport":<Integer_value>,
```

```
"autodisablegraceful":<String_value>,

"autodisabledelay":<Integer_value>,

"autodelayedtrofs":<String_value>,

"serviceipstr":<String_value>,

"servicegroupeffectivestate":<String_value>,

"monconnectionclose":<String_value>,

"nodefaultbindings":<String_value>,

"nameserver":<String_value>,

"dbsttl":<Integer_value>,

"svcitmactsvcs":<Integer_value>,

"svcitmboundsvcs":<Integer_value>,

"bootstrap":<String_value>,

"topicname":<String_value>,

"monuserstatusmesg":<String_value>,

"order":<Integer_value>,

"mcpprofilename":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/servicegroup/ servicegroupname_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/

v1/config/servicegroup/ servicegroupname_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/servicegroup/ servicegroupname_value<String> ? **view=summary**

Use this query-parameter to get the summary output of servicegroup resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "servicegroup": [ {

servicegroupname:<String_value>,includemembers:<Boolean_value>"numofconnec
tions":<Integer_value>,

"servicetype":<String_value>,

"port":<Integer_value>,

"td":<Integer_value>,

"serviceconftpye":<Boolean_value>,
```

```
"serviceconftype":<Boolean_value>,

"value":<String_value>,

"cachetype":<String_value>,

"maxclient":<Integer_value>,

"maxreq":<Integer_value>,

"cacheable":<String_value>,

"cip":<String_value>,

"cipheader":<String_value>,

"usip":<String_value>,

"pathmonitor":<String_value>,

"pathmonitorindv":<String_value>,

"useproxyport":<String_value>,

"sp":<String_value>,

"rtspsessionidremap":<String_value>,

"clttimeout":<Integer_value>,

"svrtimeout":<Integer_value>,

"cka":<String_value>,

"tcpb":<String_value>,

"cmp":<String_value>,

"maxbandwidth":<Integer_value>,

"state":<String_value>,

"svrstate":<String_value>,
```

```
"delay":<Integer_value>,

"ip":<String_value>,

"servername":<String_value>,

"monthreshold":<Integer_value>,

"weight":<Integer_value>,

"customserverid":<String_value>,

"serverid":<Integer_value>,

"monstatcode":<Integer_value>,

"monstatparam1":<Integer_value>,

"monstatparam2":<Integer_value>,

"monstatparam3":<Integer_value>,

"downstateflush":<String_value>,

"statechangetimemsec":<Integer_value>,

"timesincelaststatechange":<Integer_value>,

"stateupdatereason":<Integer_value>,

"clmonowner":<Integer_value>,

"clmonview":<Integer_value>,

"groupcount":<Integer_value>,

"comment":<String_value>,

"tcpprofilename":<String_value>,

"httpprofilename":<String_value>,

"aigwprofilename":<String_value>,
```

```
"quicprofilename":<String_value>,

"hashid":<Integer_value>,

"graceful":<String_value>,

"healthmonitor":<String_value>,

"appflowlog":<String_value>,

"netprofile":<String_value>,

"autoscale":<String_value>,

"memberport":<Integer_value>,

"autodisablegraceful":<String_value>,

"autodisabledelay":<Integer_value>,

"autodelayedtrofs":<String_value>,

"serviceipstr":<String_value>,

"servicegroupeffectivestate":<String_value>,

"monconnectionclose":<String_value>,

"nodefaultbindings":<String_value>,

"nameserver":<String_value>,

"dbsttl":<Integer_value>,

"svcitmactsvcs":<Integer_value>,

"svcitmboundsvcs":<Integer_value>,

"bootstrap":<String_value>,

"topicname":<String_value>,

"monuserstatusmesg":<String_value>,
```

```
"order":<Integer_value>,

"mcpprofilename":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/servicegroup? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "servicegroup": [ { "__count": "#no"} ] }
```

servicegroup_binding

Binding object which returns the resources bound to servicegroup.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
servicegroupname	<String>	Read-write	Name of the service group. Minimum length = 1
servicegroup_lbmonitor_binding	<servicegroup_lbmonitor_binding[]>	Read-only	lbmonitor that can be bound to servicegroup.
servicegroup_servicegroupentitymonbindings_binding	<servicegroup_servicegroupentitymonbindings_binding[]>	Read-only	servicegroupentitymonbindings that can be bound to servicegroup.
servicegroup_servicegroupmember_binding	<servicegroup_servicegroupmember_binding[]>	Read-only	servicegroupmember that can be bound to servicegroup.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.
- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/servicegroup_binding/ servicegroupname_value<String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "servicegroup_binding": [ {

"servicegroupname":<String_value>,

"servicegroup_lbmonitor_binding":<servicegroup_lbmonitor_binding[]_value>,

"servicegroup_servicegroupmember_binding":<servicegroup_servicegroupmember
_binding[]_value>,

"servicegroup_servicegroupentitymonbindings_binding":<servicegroup_service
groupentitymonbindings_binding[]_value>
```

```
}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/servicegroup_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/servicegroup_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "servicegroup_binding": [ {

"servicegroupname":<String_value>,

"servicegroup_lbmonitor_binding":<servicegroup_lbmonitor_binding[]_value>,

"servicegroup_servicegroupmember_binding":<servicegroup_servicegroupmember
_binding[]_value>,

"servicegroup_servicegroupentitymonbindings_binding":<servicegroup_service
groupentitymonbindings_binding[]_value>

}]}
```

servicegroup_lbmonitor_binding

Binding object showing the lbmonitor that can be bound to servicegroup.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
monitor_name	<String>	Read-write	Monitor name.
serverid	<Integer>	Read-write	The identifier for the service. This is used when the persistency type is set to Custom Server ID.
customserverid	<String>	Read-write	Unique service identifier. Used when the persistency type for the virtual server is set to Custom Server ID. Default value: "None"
weight	<Integer>	Read-write	Weight to assign to the servers in the service group. Specifies the capacity of the servers relative to the other servers in the load balancing configuration. The higher the weight, the higher the percentage of requests sent to the service.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum value = 1 Maximum value = 100
servicegroupname	<String>	Read-write	Name of the service group. Minimum length = 1
monstate	<String>	Read-write	Monitor state. Possible values = ENABLED, DISABLED
state	<String>	Read-write	Initial state of the service after binding. Default value: ENABLED Possible values = ENABLED, DISABLED
nameserver	<String>	Read-write	Specify the nameserver to which the query for bound domain needs to be sent. If not specified, use the global nameserver.
passive	<Boolean>	Read-write	Indicates if load monitor is passive. A passive load monitor does not remove service from LB decision when threshold is breached.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
aigwprofilename	<String>	Read-write	Name of the backend AIGW Profile which will be attached to the servicegroup. This parameter enables the servicegroup to process the LLM request/response based on the profile config. Any service item bound to the servicegroup will inherit the backend AIGW Profile bound at the servicegroup level, if it does not have an explicit AIGW Profile given at bind time. Minimum length = 1 Maximum length = 255
hashid	<Integer>	Read-write	Unique numerical identifier used by hash based load balancing methods to identify a service. Minimum value = 1
dbsttl	<Integer>	Read-write	Specify the TTL for DNS record for domain based service.The default value of ttl is 0 which indicates to use the TTL received in DNS

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			response for monitors. Default value: 0
port	<Integer>	Read-write	Port number of the service. Each service must have a unique port number. Range 1 - 65535 * in CLI is represented as 65535 in NITRO API
order	<Integer>	Read-write	Order number to be assigned to the servicegroup member. Minimum value = 1 Maximum value = 8192
monweight	<Integer>	Read-only	weight of the monitor that is bound to servicegroup.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/servicegroup_lbmonitor_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"servicegroup_lbmonitor_binding":{
```

```
<b>"servicegroupname":<String_value>,

</b>"port":<Integer_value>,

"monitor_name":<String_value>,

"monstate":<String_value>,

"passive":<Boolean_value>,

"weight":<Integer_value>,

"customserverid":<String_value>,

"serverid":<Integer_value>,

"state":<String_value>,

"hashid":<Integer_value>,

"nameserver":<String_value>,

"dbsttl":<Integer_value>,

"order":<Integer_value>,

"aigwprofilename":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/servicegroup_lbmonitor_binding/ servicegroupname_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/servicegroup_lbmonitor_binding/ servicegroupname_value<String> ? **args=port: <Integer_value> ,monitor_name: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/servicegroup_lbmonitor_binding/ servicegroupname_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/servicegroup_lbmonitor_binding/ servicegroupname_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of servicegroup_lbmonitor_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/servicegroup_lbmonitor_binding/ servicegroupname_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the servicegroup_lbmonitor_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "servicegroup_lbmonitor_binding": [ {

"monitor_name":<String_value>,

"serverid":<Integer_value>,

"customserverid":<String_value>,

"weight":<Integer_value>,

"servicegroupname":<String_value>,

"monstate":<String_value>,

"state":<String_value>,

"nameserver":<String_value>,

"passive":<Boolean_value>,

"aigwprofilename":<String_value>,

"hashid":<Integer_value>,

"dbsttl":<Integer_value>,

"port":<Integer_value>,

"order":<Integer_value>,

"monweight":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/servicegroup_lbmonitor_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/servicegroup_lbmonitor_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "servicegroup_lbmonitor_binding": [ {

"monitor_name":<String_value>,

"serverid":<Integer_value>,

"customserverid":<String_value>,

"weight":<Integer_value>,

"servicegroupname":<String_value>,

"monstate":<String_value>,

"state":<String_value>,

"nameserver":<String_value>,

"passive":<Boolean_value>,

"aigwprofilename":<String_value>,

"hashid":<Integer_value>,
```

```
"dbsttl":<Integer_value>,

"port":<Integer_value>,

"order":<Integer_value>,

"monweight":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/servicegroup_lbmonitor_binding/ servicegroupname_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"servicegroup_lbmonitor_binding": [ { "__count": "#no"} ] }
```

servicegroup_servicegroupentitymonbindings_binding

Binding object showing the servicegroupentitymonbindings that can be bound to servicegroup.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
monitor_name	<String>	Read-write	Monitor name.
servicegroupentname2	<String>	Read-write	.
customserverid	<String>	Read-write	Unique service identifier. Used when the persistency type for the virtual server is set to Custom Server ID. Default value: "None"
serverid	<Integer>	Read-write	The identifier for the service. This is used when the persistency type is set to Custom Server ID.
nameserver	<String>	Read-write	Specify the nameserver to which the query for bound domain needs to be sent. If not specified, use the global nameserver.
state	<String>	Read-write	Initial state of the service after binding. Default value: ENABLED Possible values = ENABLED, DISABLED
weight	<Integer>	Read-write	. Default value: 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum value = 1 Maximum value = 100
servicegroupname	<String>	Read-write	Name of the service group. Minimum length = 1
port	<Integer>	Read-write	Port number of the service. Each service must have a unique port number. Range 1 - 65535 * in CLI is represented as 65535 in NITRO API
dbsttl	<Integer>	Read-write	Specify the TTL for DNS record for domain based service.The default value of ttl is 0 which indicates to use the TTL received in DNS response for monitors. Default value: 0
order	<Integer>	Read-write	Order number to be assigned to the servicegroup member. Minimum value = 1 Maximum value = 8192

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
aigwprofilename	<String>	Read-write	Name of the backend AIGW Profile which will be attached to the servicegroup. This parameter enables the servicegroup to process the LLM request/response based on the profile config. Any service item bound to the servicegroup will inherit the backend AIGW Profile bound at the servicegroup level, if it does not have an explicit AIGW Profile given at bind time. Minimum length = 1 Maximum length = 255
passive	<Boolean>	Read-write	Indicates if load monitor is passive. A passive load monitor does not remove service from LB decision when threshold is breached.
hashid	<Integer>	Read-write	Unique numerical identifier used by hash based load balancing methods to identify a service. Minimum value = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
monitortotalprobes	<Integer>	Read-only	Total number of probes sent to monitor this service.
monitorcurrentfailedprobes	<Integer>	Read-only	Total number of currently failed probes.
monitortotalfailedprobes	<Integer>	Read-only	Total number of failed probes.
monitor_state	<String>	Read-only	The running state of the monitor on this service. Possible values = UP, DOWN, UNKNOWN, BUSY, OUT OF SERVICE, GOING OUT OF SERVICE, DOWN WHEN GOING OUT OF SERVICE, NS_EMPTY_STR, Unknown, DISABLED
responsetime	<Integer>	Read-only	Response time of this monitor in milli sec.
lastresponse	<String>	Read-only	The string form of monstatcode.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET

- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/ servicegroup_servicegroupentitymonbindings_binding/ servicegroupname_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ servicegroup_servicegroupentitymonbindings_binding/ servicegroupname_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of servicegroup_servicegroupentitymonbindings_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ servicegroup_servicegroupentitymonbindings_binding/ servicegroupname_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the servicegroup_servicegroupentitymonbindings_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "servicegroup_servicegroupentitymonbindings_binding": [ {

"monitor_name":<String_value>,

"servicegroupentname2":<String_value>,

"customserverid":<String_value>,

"serverid":<Integer_value>,

"nameserver":<String_value>,

"state":<String_value>,

"weight":<Integer_value>,

"servicegroupname":<String_value>,
```

```
"port":<Integer_value>,

"dbsttl":<Integer_value>,

"order":<Integer_value>,

"aigwprofilename":<String_value>,

"passive":<Boolean_value>,

"hashid":<Integer_value>,

"monitortotalprobes":<Integer_value>,

"monitorcurrentfailedprobes":<Integer_value>,

"monitortotalfailedprobes":<Integer_value>,

"monitor_state":<String_value>,

"responsetime":<Integer_value>,

"lastresponse":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/ servicegroup_servicegroupentitymonbindings_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ servicegroup_servicegroupentitymonbindings_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "servicegroup_servicegroupentitymonbindings_binding": [ {

"monitor_name":<String_value>,

"servicegroupentname2":<String_value>,

"customserverid":<String_value>,

"serverid":<Integer_value>,

"nameserver":<String_value>,

"state":<String_value>,

"weight":<Integer_value>,

"servicegroupname":<String_value>,

"port":<Integer_value>,

"dbsttl":<Integer_value>,

"order":<Integer_value>,

"aigwprofilename":<String_value>,

"passive":<Boolean_value>,

"hashid":<Integer_value>,

"monitortotalprobes":<Integer_value>,

"monitorcurrentfailedprobes":<Integer_value>,
```

```
"monitortotalfailedprobes":<Integer_value>,

"monitor_state":<String_value>,

"responsetime":<Integer_value>,

"lastresponse":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/ servicegroup_servicegroupentitymonbindings_binding/ servicegroupname_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"servicegroup_servicegroupentitymonbindings_binding": [ { "__count":
"#no"} ] }
```

servicegroup_servicegroupmember_binding

Binding object showing the servicegroupmember that can be bound to servicegroup.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
serverid	<Integer>	Read-write	The identifier for the service. This is used when the persistency type is set to Custom Server ID.
customserverid	<String>	Read-write	The identifier for this IP:Port pair. Used when the persistency type is set to Custom Server ID. Default value: "None"
aigwprofilename	<String>	Read-write	Name of the backend AIGW Profile which will be attached to the servicegroup. This parameter enables the servicegroup to process the LLM request/response based on the profile config. Any service item bound to the servicegroup will inherit the backend AIGW Profile bound at the servicegroup level, if it does not have an explicit AIGW Profile given at bind time. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum length = 255
hashid	<Integer>	Read-write	The hash identifier for the service. This must be unique for each service. This parameter is used by hash based load balancing methods. Minimum value = 1
dbsttl	<Integer>	Read-write	Specify the TTL for DNS record for domain based service.The default value of ttl is 0 which indicates to use the TTL received in DNS response for monitors. Default value: 0
port	<Integer>	Read-write	Server port number. Range 1 - 65535 * in CLI is represented as 65535 in NITRO API
order	<Integer>	Read-write	Order number to be assigned to the servicegroup member. Minimum value = 1 Maximum value = 8192

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ip	<String>	Read-write	IP Address.
weight	<Integer>	Read-write	Weight to assign to the servers in the service group. Specifies the capacity of the servers relative to the other servers in the load balancing configuration. The higher the weight, the higher the percentage of requests sent to the service. Minimum value = 1 Maximum value = 100
servername	<String>	Read-write	Name of the server to which to bind the service group. Minimum length = 1
servicegroupname	<String>	Read-write	Name of the service group. Minimum length = 1
state	<String>	Read-write	Initial state of the service group. Default value: ENABLED Possible values = ENABLED, DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
nameserver	<String>	Read-write	Specify the nameserver to which the query for bound domain needs to be sent. If not specified, use the global nameserver.
trofsreason	<String>	Read-only	Specify reason if service group member in TROFS. Possible values = Trofs Because of Graceful Unbind, Trofs Because of Disable Cmd, Trofs Becasue of Autoscale IP not present in DNS Response, Trofs Because of Monitor Response has Trofs String
graceful	<String>	Read-only	Wait for all existing connections to the service to terminate before shutting down the service. Default value: NO Possible values = YES, NO
delay	<Integer>	Read-only	Time, in seconds, allocated for a shutdown of the services in the service group.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			During this period, new requests are sent to the service only for clients who already have persistent sessions on the appliance. Requests from new clients are load balanced among other available services. After the delay time expires, no requests are sent to the service, and the service is marked as unavailable (OUT OF SERVICE).
svrstate	<String>	Read-only	The state of the service. Possible values = UP, DOWN, UNKNOWN, BUSY, OUT OF SERVICE, GOING OUT OF SERVICE, DOWN WHEN GOING OUT OF SERVICE, NS_EMPTY_STR, Unknown, DISABLED
trofsdelay	<Integer>	Read-only	Delay before moving to TROFS.
svcitmpriority	<Integer>	Read-only	This gives the priority of the FQDN service

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			items for SRV server binding.
statechangetimesec	<String>	Read-only	Time when last state change occurred. Seconds part.
orderstr	<String>	Read-only	Order number in string form to be assigned to the servicegroup member.
tickssincelaststatechange	<Integer>	Read-only	Time in 10 millisecond ticks since the last state change.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/servicegroup_servicegroupmember_binding
HTTP Method: PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"servicegroup_servicegroupmember_binding":{

<b>"servicegroupname":<String_value>,

</b>"ip":<String_value>,

"servername":<String_value>,

"port":<Integer_value>,

"weight":<Integer_value>,
```

```
"customserverid":<String_value>,

"serverid":<Integer_value>,

"state":<String_value>,

"hashid":<Integer_value>,

"nameserver":<String_value>,

"dbsttl":<Integer_value>,

"order":<Integer_value>,

"aigwprofilename":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/servicegroup_servicegroupmember_binding/ servicegroupname_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/servicegroup_servicegroupmember_binding/ servicegroupname_value<String> ? **args=ip: <String_value> ,servername: <String_value> ,port: <Integer_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/servicegroup_servicegroupmember_binding/ servicegroupname_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/servicegroup_servicegroupmember_binding/ servicegroupname_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of servicegroup_servicegroupmember_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ servicegroup_servicegroupmember_binding/ servicegroupname_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the servicegroup_servicegroupmember_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "servicegroup_servicegroupmember_binding": [ {

"serverid":<Integer_value>,

"customserverid":<String_value>,

"aigwprofilename":<String_value>,

"hashid":<Integer_value>,
```

```
"dbsttl":<Integer_value>,

"port":<Integer_value>,

"order":<Integer_value>,

"ip":<String_value>,

"weight":<Integer_value>,

"servername":<String_value>,

"servicegroupname":<String_value>,

"state":<String_value>,

"nameserver":<String_value>,

"trofsreason":<String_value>,

"graceful":<String_value>,

"delay":<Integer_value>,

"svrstate":<String_value>,

"trofsdelay":<Integer_value>,

"svcitmpriority":<Integer_value>,

"statechangetimesec":<String_value>,

"orderstr":<String_value>,

"tickssincelaststatechange":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/servicegroup_servicegroupmember_binding

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ servicegroup_servicegroupmember_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "servicegroup_servicegroupmember_binding": [ {

"serverid":<Integer_value>,

"customserverid":<String_value>,

"aigwprofilename":<String_value>,

"hashid":<Integer_value>,

"dbsttl":<Integer_value>,

"port":<Integer_value>,

"order":<Integer_value>,

"ip":<String_value>,

"weight":<Integer_value>,
```

```
"servername":<String_value>,

"servicegroupname":<String_value>,

"state":<String_value>,

"nameserver":<String_value>,

"trofsreason":<String_value>,

"graceful":<String_value>,

"delay":<Integer_value>,

"svrstate":<String_value>,

"trofsdelay":<Integer_value>,

"svcitmpriority":<Integer_value>,

"statechangetimesec":<String_value>,

"orderstr":<String_value>,

"tickssincelaststatechange":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/servicegroup_servicegroupmember_binding/servicegroupname_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"servicegroup_servicegroupmember_binding": [ { "__count": "#no"} ] }
```

servicegroup_servicegroupmemberlist_binding

Binding object showing the servicegroupmemberlist that can be bound to servicegroup.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
members	<object[]>	Read-write	Desired servicegroupmember binding set. Any existing servicegroupmember which is not part of the input will be deleted or disabled based on graceful setting on servicegroup.
servicegroupname	<String>	Read-write	Name of the service group. Minimum length = 1
failedmembers	<object[]>	Read-only	List of servicegroupmembers which couldn't be bound.

OBJECT MEMBER	NAME	TYPE	DESCRIPTION
	ip port weight state order	<String> <Integer> <Integer> <String> <Integer>	IP Address. The port number of the service to be enabled. Range 1 - 65535 * in CLI is represented as 65535 in NITRO API . Default value: 1 Minimum value = 1 Maximum value = 100 Initial state of the service group. Default value: ENABLED Possible values = ENABLED, DISABLED Order number to be assigned to the servicegroup member. Minimum value = 1 Maximum value = 8192
	ip port	<String> <Integer>	IP Address. The port number of the service to be enabled. Range 1 - 65535 * in CLI is represented as 65535 in NITRO API

Operations

(click to see Properties)

- ADD
- DELETE

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/servicegroup_servicegroupmemberlist_binding
HTTP Method: PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"servicegroup_servicegroupmemberlist_binding":{

<b>"servicegroupname":<String_value>,

</b>"members":<object[]_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/servicegroup_servicegroupmemberlist_binding/servicegroupname_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

servicegroupbindings

Configuration for servicegroupbind resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
servicegroupname	<String>	Read-write	The name of the service. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ipaddress	<String>	Read-only	The IP address of the vserver.
port	<Integer>	Read-only	The port of the vserver. Range 1 - 65535 * in CLI is represented as 65535 in NITRO API
state	<String>	Read-only	The state of the service group. Possible values = ENABLED, DISABLED
svrstate	<String>	Read-only	The state of the vserver. Possible values = UP, DOWN, UNKNOWN, BUSY, OUT OF SERVICE, GOING OUT OF SERVICE, DOWN WHEN GOING OUT OF SERVICE, NS_EMPTY_STR, Unknown, DISABLED
vservername	<String>	Read-only	The name of the vserver.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/servicegroupbindings **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/servicegroupbindings? **args= servicegroupname:<String_value>,**

Use this query-parameter to get servicegroupbindings resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/config/servicegroupbindings? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/servicegroupbindings? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of servicegroupbindings resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/servicegroupbindings? **view=summary**

Use this query-parameter to get the summary output of servicegroupbindings resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/servicegroupbindings? **pagesize=#no;pageno=#no**

Use this query-parameter to get the servicegroupbindings resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "servicegroupbindings": [ {

<b>servicegroupname:<String_value>,</b>"ipaddress":<String_value>,
```

```
"port":<Integer_value>,

"state":<String_value>,

"svrstate":<String_value>,

"vservername":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/servicegroupbindings/ servicegroupname_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/servicegroupbindings/ servicegroupname_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/servicegroupbindings/ servicegroupname_value<String> ? **view=summary**

Use this query-parameter to get the summary output of servicegroupbindings resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "servicegroupbindings": [ {

<b>servicegroupname:<String_value>,</b>"ipaddress":<String_value>,

"port":<Integer_value>,

"state":<String_value>,

"svrstate":<String_value>,

"vservername":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/servicegroupbindings? **args= servicegroupname:<String_value>, ;count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "servicegroupbindings": [ { "__count": "#no"} ] }
```

svcbindings

Configuration for service bindings resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
servicename	<String>	Read-write	The name of the service. Minimum length = 1
ipaddress	<String>	Read-only	The IP address of the vserver.
port	<Integer>	Read-only	The port of the vserver. Range 1 - 65535 * in CLI is represented as 65535 in NITRO API
svrstate	<String>	Read-only	The state of the vserver. Possible values = UP, DOWN, UNKNOWN, BUSY, OUT OF SERVICE, GOING OUT OF SERVICE, DOWN WHEN GOING OUT OF SERVICE, NS_EMPTY_STR,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Unknown, DISABLED
vservername	<String>	Read-only	The name of the vserver.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/svcbindings **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/svcbindings? **args= servicename:<String_value>,**

Use this query-parameter to get svcbindings resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/config/svcbindings? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/svcbindings? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of svcbindings resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/svcbindings? **view=summary**

Use this query-parameter to get the summary output of svcbindings resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/svcbindings? **pagesize=#no;pageno=#no**

Use this query-parameter to get the svcbindings resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "svcbindings": [ {

<b>servicename:<String_value>,</b>"ipaddress":<String_value>,

"port":<Integer_value>,

"svrstate":<String_value>,

"vservername":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/svcbindings/ servicename_value<String>
Query-parameters: attrs http:// <netscaler-ip-address> /nitro/v1/config/svcbindings/ servicename_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/svcbindings/ servicename_value<String> ? **view=summary**

Use this query-parameter to get the summary output of svcbindings resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "svcbindings": [ {

<b>servicename:<String_value>,</b>"ipaddress":<String_value>,

"port":<Integer_value>,

"svrstate":<String_value>,

"vservername":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/svcbindings? **args= servicename:<String_value>, ;count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "svcbindings": [ { "__count": "#no"} ] }
```

vserver

Configuration for virtual server resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	The name of the virtual server to be removed. Minimum length = 1
backupvserver	<String>	Read-write	The name of the backup virtual server for this virtual server. Minimum length = 1
redirecturl	<String>	Read-write	The URL where traffic is redirected if the virtual server in the system becomes unavailable. Minimum length = 1
cacheable	<String>	Read-write	Use this option to specify whether a virtual server (used for load balancing or content switching) routes requests to the cache redirection virtual server before sending it to the configured servers.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = YES, NO
clttimeout	<Integer>	Read-write	The timeout value in seconds for idle client connection. Minimum value = 0 Maximum value = 31536000
somethod	<String>	Read-write	The spillover factor. The system will use this value to determine if it should send traffic to the backupvserver when the main virtual server reaches the spillover threshold. Possible values = CONNECTION, DYNAMICCONNECTION, BANDWIDTH, HEALTH, LLMQUOTA, NONE
sopersistence	<String>	Read-write	The state of the spillover persistence. Default value: DISABLED Possible values = ENABLED, DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
sopersistencetimeout	<Integer>	Read-write	The spillover persistence entry timeout. Default value: 2 Minimum value = 2 Maximum value = 1440
sothreshold	<Integer>	Read-write	The spillver threshold value. Minimum value = 1 Maximum value = 4294967294
pushvserver	<String>	Read-write	The lb vserver of type PUSH/ SSL_PUSH to which server pushes the updates received on the client facing non-push lb vserver. Minimum length = 1

Operations

(click to see Properties)

- DELETE
- UPDATE
- ENABLE
- DISABLE

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vserver/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vserver **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"vserver":{

<b>"name":<String_value>,

</b>"backupvserver":<String_value>,

"redirecturl":<String_value>,

"cacheable":<String_value>,

"clttimeout":<Integer_value>,

"somethod":<String_value>,

"sopersistence":<String_value>,

"sopersistencetimeout":<Integer_value>,

"sothreshold":<Integer_value>,

"pushvserver":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

ENABLE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vserver? **action=enable HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"vserver":{

<b>"name":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DISABLE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vserver? **action=disable HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"vserver":{

<b>"name":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

bfd

Bfd

Bidirectional Forwarding Detection

NAME	DESCRIPTION
bfdsession	Configuration for BFD configuration

bfdsession

Configuration for BFD configuration resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
localip	<String>	Read-write	IPV4 or IPV6 Address of Local Node.
remoteip	<String>	Read-write	IPV4 or IPV6 Address of Remote Node.
state	<String>	Read-only	Current state of the BFD session. Possible values = ADMIN DOWN, DOWN, INIT, UP
localport	<Integer>	Read-only	Source Port used by Local node to send Control packets for the BFD session.
remoteport	<Integer>	Read-only	Source Port used by Remote node to send Control packets for the BFD session.
minimumtransmitinterval	<Integer>	Read-only	Minimum trasmit interval, in milliseconds, the local node would like to use when

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			transmitting BFD Control packets.
negotiatedminimumtransmitinterval	<Integer>	Read-only	Negotiated Minimum Transmit Interval. This is the interval at which the local node will be sending out BFD control packets.
minimumreceiveinterval	<Integer>	Read-only	Minimum receive interval, in milliseconds, between received BFD Control packets that the local node is capable of supporting.
negotiatedminimumreceiveinterval	<Integer>	Read-only	Negotiated Minimum Receive Interval. This is the interval at which the local node will be expecting BFD control packets.
multiplier	<Integer>	Read-only	Detection Multiplier. The negotiated transmit interval multiplied by Detection multiplier provides the Detection Time for the remote node for the BFD session.
remotemultiplier	<Integer>	Read-only	Your Multiplier. The negotiated receive interval multiplied by Your Multiplier provides the Detection Time for

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			the local node for the BFD session.
vlan	<Integer>	Read-only	VLAN ID on which the BDS session is configured.
localdiagnotic	<Integer>	Read-only	Diagnostic Code specifying the local system's reason for the last change in session state.
localdiscriminator	<Integer>	Read-only	A unique discriminator value generated by the local node for the session.
remotediscriminator	<Integer>	Read-only	A unique discriminator value as received from the remote node for the session.
passive	<Boolean>	Read-only	Flag indicating that the session is passive.
multihop	<Boolean>	Read-only	Flag indicating if the session is multihop.
admindown	<Boolean>	Read-only	Flag indicating if admin down is being sent.
originalownerpe	<Integer>	Read-only	Original Owner PE of the BFD session.
currentownerpe	<Integer>	Read-only	Current Owner PE of the BFD session.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ownernode	<Integer>	Read-only	The owner node in a Cluster for this BFD session. Owner node can vary from 0 to 31. If ownernode is not specified then the session is treated as Striped session. Default value: 255
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/bfdsession **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/bfdsession? **args=localip: <String_value> ,remoteip: <String_value>**

Use this query-parameter to get bfdsession resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/config/bfdsession? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/bfdsession? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of bfdsession resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/bfdsession? **view=summary**

Use this query-parameter to get the summary output of bfdsession resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/bfdsession? **pagesize=#no;pageno=#no**

Use this query-parameter to get the bfdsession resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "bfdsession": [ {

localip:<String_value>,remoteip:<String_value>"state":<String_value>,

"localport":<Integer_value>,

"remoteport":<Integer_value>,

"minimumtransmitinterval":<Integer_value>,

"negotiatedminimumtransmitinterval":<Integer_value>,

"minimumreceiveinterval":<Integer_value>,

"negotiatedminimumreceiveinterval":<Integer_value>,

"multiplier":<Integer_value>,

"remotemultiplier":<Integer_value>,

"vlan":<Integer_value>,

"localdiagnotic":<Integer_value>,

"localdiscriminator":<Integer_value>,

"remotediscriminator":<Integer_value>,

"passive":<Boolean_value>,

"multihop":<Boolean_value>,

"admindown":<Boolean_value>,
```

```
"originalownerpe":<Integer_value>,

"currentownerpe":<Integer_value>,

"ownernode":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/bfdsession? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "bfdsession": [ { "__count": "#no"} ] }
```

bot

Bot

Bot Management.

NAME	DESCRIPTION
botglobal_binding	Binding object showing the resources that can be bound to botglobal
botglobal_botpolicy_binding	Binding object showing the botpolicy that can be bound to botglobal
botpolicy	Configuration for Bot policy
botpolicy_binding	Binding object showing the resources that can be bound to botpolicy
botpolicy_botglobal_binding	Binding object showing the botglobal that can be bound to botpolicy
botpolicy_botpolicylabel_binding	Binding object showing the botpolicylabel that can be bound to botpolicy
botpolicy_csvserver_binding	Binding object showing the csvserver that can be bound to botpolicy
botpolicy_lbvserver_binding	Binding object showing the lbvserver that can be bound to botpolicy
botpolicylabel	Configuration for Bot policy label
botpolicylabel_binding	Binding object showing the resources that can be bound to botpolicylabel
botpolicylabel_botpolicy_binding	Binding object showing the botpolicy that can be bound to botpolicylabel

NAME	DESCRIPTION
botpolicylabel_policybinding_binding	Binding object showing the policybinding that can be bound to botpolicylabel
botprofile	Configuration for Bot profile
botprofile_binding	Binding object showing the resources that can be bound to botprofile
botprofile_blacklist_binding	Binding object showing the blacklist that can be bound to botprofile
botprofile_captcha_binding	Binding object showing the captcha that can be bound to botprofile
botprofile_ipreputation_binding	Binding object showing the ipreputation that can be bound to botprofile
botprofile_kmdetectionexpr_binding	Binding object showing the kmdetectionexpr that can be bound to botprofile
botprofile_logexpression_binding	Binding object showing the logexpression that can be bound to botprofile
botprofile_ratelimit_binding	Binding object showing the ratelimit that can be bound to botprofile
botprofile_tps_binding	Binding object showing the tps that can be bound to botprofile
botprofile_trapinsertionurl_binding	Binding object showing the trapinsertionurl that can be bound to botprofile

NAME	DESCRIPTION
botprofile_whitelist_binding	Binding object showing the whitelist that can be bound to botprofile
botsettings	Configuration for Bot engine settings
botsignature	Configuration for bot signatures

botglobal_binding

Binding object which returns the resources bound to botglobal.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
botglobal_botpolicy_binding	<botglobal_botpolicy_binding[]>	Read-write	botpolicy that can be bound to botglobal.

Operations

(click to see Properties)

- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of

creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/botglobal_binding

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "botglobal_binding": [ {

"botglobal_botpolicy_binding":<botglobal_botpolicy_binding[]_value>

}]}
```

botglobal_botpolicy_binding

Binding object showing the botpolicy that can be bound to botglobal.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
type	<String>	Read-write	Specifies the bind point whose policies you want to display. Available settings function as follows: * REQ_OVERRIDE - Request override. Binds the policy to the priority request queue. * REQ_DEFAULT - Binds the policy to the default request queue. Possible values = REQ_OVERRIDE, REQ_DEFAULT
globalbindtype	<String>	Read-write	. Default value: SYSTEM_GLOBAL Possible values = SYSTEM_GLOBAL, VPN_GLOBAL, RNAT_GLOBAL, APPFW_GLOBAL, TM_GLOBAL

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
policyname	<String>	Read-write	Name of the bot policy.
gotopriorityexpression	<String>	Read-write	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
invoke	<Boolean>	Read-write	If the current policy evaluates to TRUE, terminate evaluation of policies bound to the current policy label, and then forward the request to the specified virtual server.
labeltype	<String>	Read-write	Type of invocation, Available settings function as follows: * vserver - Forward the request to the specified virtual server. * policylabel - Invoke the specified policy label. Possible values = vserver, policylabel
priority	<Integer>	Read-write	Specifies the priority of the policy.
labelname	<String>	Read-write	Name of the policy label to invoke. If the current policy evaluates to TRUE, the invoke parameter

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			is set, and Label Type is policylabel.
flowtype	<Integer>	Read-only	flowtype of the bound bot policy.
numpol	<Integer>	Read-only	number of polices bound to label.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/botglobal_botpolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"botglobal_botpolicy_binding":{

<b>"policyname":<String_value>,

</b><b>"priority":<Integer_value>,

</b>"gotopriorityexpression":<String_value>,

"type":<String_value>,

"invoke":<Boolean_value>,

"labeltype":<String_value>,

"labelname":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/botglobal_botpolicy_binding **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/botglobal_botpolicy_binding? **args= policyname:<String_value>, type: <String_value> ,priority: <Integer_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/botglobal_botpolicy_binding **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/botglobal_botpolicy_binding? **args=type: <String_value>**

Use this query-parameter to get botglobal_botpolicy_binding resources based on additional properties.

filter http:// <netscaler-ip-address> /nitro/v1/config/botglobal_botpolicy_binding? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of botglobal_botpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/botglobal_botpolicy_binding? **pagesize=#no;pageno=#no**

Use this query-parameter to get the botglobal_botpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "botglobal_botpolicy_binding": [ {

"type":<String_value>,

"globalbindtype":<String_value>,

"policyname":<String_value>,

"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"labelname":<String_value>,

"flowtype":<Integer_value>,

"numpol":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/botglobal_botpolicy_binding? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "botglobal_botpolicy_binding": [ { "__count": "#no"} ] }
```

botpolicy

Configuration for Bot policy resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the bot policy. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Can be changed after the bot policy is added.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my bot policy" or 'my bot policy').
rule	<String>	Read-write	Expression that the policy uses to determine whether to apply bot profile on the specified request.
profilename	<String>	Read-write	Name of the bot profile to apply if the request matches this bot policy.
undefaction	<String>	Read-write	Action to perform if the result of policy evaluation is undefined (UNDEF). An UNDEF event indicates an internal error condition.
comment	<String>	Read-write	Any type of information about this bot policy.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
logaction	<String>	Read-write	Name of the messagelog action to use for requests that match this policy.
newname	<String>	Read-write	New name for the bot policy. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space ( ), at (@), equals (=), colon (:), and underscore characters. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my bot policy" or 'my bot policy'). Minimum length = 1
hits	<Integer>	Read-only	Number of hits.
undefhits	<Integer>	Read-only	Number of policy UNDEF hits.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
builtin	<String[]>	Read-only	Flag to determine if bot policy is built-in or not. Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL
feature	<String>	Read-only	The feature to be checked while applying this config.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT
- RENAME

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/botpolicy **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"botpolicy":{

<b>"name":<String_value>,

</b><b>"rule":<String_value>,

</b><b>"profilename":<String_value>,

</b>"undefaction":<String_value>,

"comment":<String_value>,

"logaction":<String_value>
```

```
}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/botpolicy/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/botpolicy **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"botpolicy":{

<b>"name":<String_value>,

</b>"rule":<String_value>,

"profilename":<String_value>,

"undefaction":<String_value>,

"comment":<String_value>,
```

```
"logaction":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/botpolicy? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"botpolicy":{

<b>"name":<String_value>,

</b>"undefaction":true,

"comment":true,

"logaction":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

RENAME

URL: http:// <netscaler-ip-address> /nitro/v1/config/botpolicy? **action=rename HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"botpolicy":{

<b>"name":<String_value>,

</b><b>"newname":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/botpolicy **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/botpolicy? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/botpolicy? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of botpolicy resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/botpolicy? **view=summary**

Use this query-parameter to get the summary output of botpolicy resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/botpolicy? **pagesize=#no;pageno=#no**

Use this query-parameter to get the botpolicy resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "botpolicy": [ {

"name":<String_value>,

"rule":<String_value>,

"profilename":<String_value>,

"undefaction":<String_value>,

"hits":<Integer_value>,

"undefhits":<Integer_value>,

"comment":<String_value>,

"logaction":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/botpolicy/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/botpolicy/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/botpolicy/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of botpolicy resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "botpolicy": [ {

"name":<String_value>,

"rule":<String_value>,

"profilename":<String_value>,
```

```
"undefaction":<String_value>,

"hits":<Integer_value>,

"undefhits":<Integer_value>,

"comment":<String_value>,

"logaction":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/botpolicy? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "botpolicy": [ { "__count": "#no"} ] }
```

botpolicy_binding

Binding object which returns the resources bound to botpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the bot policy for which to display settings.
botpolicy_botglobal_binding	<botpolicy_botglobal_binding[]>	Read-only	botglobal that can be bound to botpolicy.
botpolicy_lbvserver_binding	<botpolicy_lbvserver_binding[]>	Read-only	lbvserver that can be bound to botpolicy.
botpolicy_csvserver_binding	<botpolicy_csvserver_binding[]>	Read-only	csvserver that can be bound to botpolicy.
botpolicy_botpolicylabel_binding	<botpolicy_botpolicylabel_binding[]>	Read-only	botpolicylabel that can be bound to botpolicy.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/botpolicy_binding/ name_value<String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "botpolicy_binding": [ {

"name":<String_value>,

"botpolicy_botpolicylabel_binding":<botpolicy_botpolicylabel_binding[]_val
ue>,
```

```
"botpolicy_lbvserver_binding":<botpolicy_lbvserver_binding[]_value>,

"botpolicy_csvserver_binding":<botpolicy_csvserver_binding[]_value>,

"botpolicy_botglobal_binding":<botpolicy_botglobal_binding[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/botpolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/botpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "botpolicy_binding": [ {

"name":<String_value>,

"botpolicy_botpolicylabel_binding":<botpolicy_botpolicylabel_binding[]_val
ue>,
```

```
"botpolicy_lbvserver_binding":<botpolicy_lbvserver_binding[]_value>,

"botpolicy_csvserver_binding":<botpolicy_csvserver_binding[]_value>,

"botpolicy_botglobal_binding":<botpolicy_botglobal_binding[]_value>

}]}
```

botpolicy_botglobal_binding

Binding object showing the botglobal that can be bound to botpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the bot policy for which to display settings.
boundto	<String>	Read-write	Location where policy is bound.
labelname	<String>	Read-only	Name of the label to invoke if the current policy rule evaluates to TRUE.
gotopriorityexpression	<String>	Read-only	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
activepolicy	<Integer>	Read-only	Indicates whether policy is bound or not.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
labeltype	<String>	Read-only	Type of policy label invocation. Possible values = reqvserver, resvserver, policylabel
priority	<Integer>	Read-only	Specifies the priority of the policy.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/botpolicy_botglobal_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ botpolicy_botglobal_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of botpolicy_botglobal_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/botpolicy_botglobal_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the botpolicy_botglobal_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "botpolicy_botglobal_binding": [ {

"name":<String_value>,
```

```
"boundto":<String_value>,

"labelname":<String_value>,

"gotopriorityexpression":<String_value>,

"activepolicy":<Integer_value>,

"labeltype":<String_value>,

"priority":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/botpolicy_botglobal_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/botpolicy_botglobal_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "botpolicy_botglobal_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"labelname":<String_value>,

"gotopriorityexpression":<String_value>,

"activepolicy":<Integer_value>,

"labeltype":<String_value>,

"priority":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/botpolicy_botglobal_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"botpolicy_botglobal_binding": [ { "__count": "#no"} ] }
```

botpolicy_botpolicylabel_binding

Binding object showing the botpolicylabel that can be bound to botpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the bot policy for which to display settings.
boundto	<String>	Read-write	Location where policy is bound.
labeltype	<String>	Read-only	Type of policy label invocation. Possible values = reqvserver, resvserver, policylabel
priority	<Integer>	Read-only	Specifies the priority of the policy.
labelname	<String>	Read-only	Name of the label to invoke if the current policy rule evaluates to TRUE.
gotopriorityexpression	<String>	Read-only	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
activepolicy	<Integer>	Read-only	Indicates whether policy is bound or not.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/botpolicy_botpolicylabel_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ botpolicy_botpolicylabel_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of botpolicy_botpolicylabel_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/botpolicy_botpolicylabel_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the botpolicy_botpolicylabel_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "botpolicy_botpolicylabel_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"labelname":<String_value>,
```

```
"gotopriorityexpression":<String_value>,

"activepolicy":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/botpolicy_botpolicylabel_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/botpolicy_botpolicylabel_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "botpolicy_botpolicylabel_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"labeltype":<String_value>,
```

```
"priority":<Integer_value>,

"labelname":<String_value>,

"gotopriorityexpression":<String_value>,

"activepolicy":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/botpolicy_botpolicylabel_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"botpolicy_botpolicylabel_binding": [ { "__count": "#no"} ] }
```

botpolicy_csvserver_binding

Binding object showing the csvserver that can be bound to botpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
boundto	<String>	Read-write	Location where policy is bound.
name	<String>	Read-write	Name of the bot policy for which to display settings.
priority	<Integer>	Read-only	Specifies the priority of the policy.
labeltype	<String>	Read-only	Type of policy label invocation. Possible values = reqvserver, resvserver, policylabel
activepolicy	<Integer>	Read-only	Indicates whether policy is bound or not.
gotopriorityexpression	<String>	Read-only	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
labelname	<String>	Read-only	Name of the label to invoke if the current policy rule evaluates to TRUE.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET

- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/botpolicy_csvserver_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ botpolicy_csvserver_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of botpolicy_csvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/botpolicy_csvserver_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the botpolicy_csvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "botpolicy_csvserver_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"priority":<Integer_value>,

"labeltype":<String_value>,

"activepolicy":<Integer_value>,

"gotopriorityexpression":<String_value>,

"labelname":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/botpolicy_csvserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ botpolicy_csvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "botpolicy_csvserver_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"priority":<Integer_value>,

"labeltype":<String_value>,

"activepolicy":<Integer_value>,

"gotopriorityexpression":<String_value>,

"labelname":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/botpolicy_csvserver_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"botpolicy_csvserver_binding": [ { "__count": "#no"} ] }
```

botpolicy_lbvserver_binding

Binding object showing the lbvserver that can be bound to botpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
boundto	<String>	Read-write	Location where policy is bound.
name	<String>	Read-write	Name of the bot policy for which to display settings.
labelname	<String>	Read-only	Name of the label to invoke if the current

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			policy rule evaluates to TRUE.
gotopriorityexpression	<String>	Read-only	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
activepolicy	<Integer>	Read-only	Indicates whether policy is bound or not.
labeltype	<String>	Read-only	Type of policy label invocation. Possible values = reqvserver, resvserver, policylabel
priority	<Integer>	Read-only	Specifies the priority of the policy.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/botpolicy_lbvserver_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ botpolicy_lbvserver_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of botpolicy_lbvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/botpolicy_lbvserver_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the botpolicy_lbvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "botpolicy_lbvserver_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"labelname":<String_value>,

"gotopriorityexpression":<String_value>,

"activepolicy":<Integer_value>,

"labeltype":<String_value>,

"priority":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/botpolicy_lbvserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/botpolicy_lbvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "botpolicy_lbvserver_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"labelname":<String_value>,

"gotopriorityexpression":<String_value>,

"activepolicy":<Integer_value>,

"labeltype":<String_value>,

"priority":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/botpolicy_lbvserver_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"botpolicy_lbvserver_binding": [ { "__count": "#no"} ] }
```

botpolicylabel

Configuration for Bot policy label resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
labelname	<String>	Read-write	Name for the bot policy label. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after the responder policy label is added.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my responder policy label" or my responder policy label').
comment	<String>	Read-write	Any comments to preserve information about this bot policy label.
newname	<String>	Read-write	New name for the bot policy label. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Minimum length = 1
numpol	<Integer>	Read-only	number of polices bound to label.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
hits	<Integer>	Read-only	Number of times policy label was invoked.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET (ALL)
- GET
- COUNT
- RENAME

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/botpolicylabel **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"botpolicylabel":{

<b>"labelname":<String_value>,

</b>"comment":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/botpolicylabel/ labelname_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

RENAME

URL: http:// <netscaler-ip-address> /nitro/v1/config/botpolicylabel? **action=rename HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"botpolicylabel":{

<b>"labelname":<String_value>,

</b><b>"newname":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/botpolicylabel **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/botpolicylabel? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/botpolicylabel? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of botpolicylabel resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/botpolicylabel? **view=summary**

Use this query-parameter to get the summary output of botpolicylabel resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/botpolicylabel? **pagesize=#no;pageno=#no**

Use this query-parameter to get the botpolicylabel resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "botpolicylabel": [ {

"labelname":<String_value>,

"numpol":<Integer_value>,

"hits":<Integer_value>,

"comment":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/botpolicylabel/ labelname_value<String>
Query-parameters: attrs http:// <netscaler-ip-address> /nitro/v1/config/botpolicylabel/ labelname_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/botpolicylabel/ labelname_value<String> ? **view=summary**

Use this query-parameter to get the summary output of botpolicylabel resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "botpolicylabel": [ {

"labelname":<String_value>,

"numpol":<Integer_value>,

"hits":<Integer_value>,

"comment":<String_value>,
```

```
"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/botpolicylabel? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "botpolicylabel": [ { "__count": "#no"} ] }
```

botpolicylabel_binding

Binding object which returns the resources bound to botpolicylabel.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
labelname	<String>	Read-write	Name of the bot policy label.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
botpolicylabel_policybinding_binding	<botpolicylabel_policybinding_binding[]>	Read-only	policybinding that can be bound to botpolicylabel.
botpolicylabel_botpolicy_binding	<botpolicylabel_botpolicy_binding[]>	Read-only	botpolicy that can be bound to botpolicylabel.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/botpolicylabel_binding/ labelname_value<String>

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "botpolicylabel_binding": [ {

"labelname":<String_value>,

"botpolicylabel_policybinding_binding":<botpolicylabel_policybinding_binding[]_value>,

"botpolicylabel_botpolicy_binding":<botpolicylabel_botpolicy_binding[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/botpolicylabel_binding

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters:

bulkbindings

http:// <netscaler-ip-address> /nitro/v1/config/botpolicylabel_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "botpolicylabel_binding": [ {

"labelname":<String_value>,

"botpolicylabel_policybinding_binding":<botpolicylabel_policybinding_binding[]_value>,

"botpolicylabel_botpolicy_binding":<botpolicylabel_botpolicy_binding[]_value>

}]}
```

botpolicylabel_botpolicy_binding

Binding object showing the botpolicy that can be bound to botpolicylabel.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
labelname	<String>	Read-write	Name of the bot policy label to which to bind the policy.
labeltype	<String>	Read-write	Type of policy label to invoke. Available settings function as follows: * vserver - Invoke an unnamed policy label associated with a virtual server. * policylabel - Invoke a user-defined policy label. Possible values = vserver, policylabel
priority	<Integer>	Read-write	Specifies the priority of the policy.
gotopriorityexpression	<String>	Read-write	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
invoke	<Boolean>	Read-write	If the current policy evaluates to TRUE, terminate evaluation

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			of policies bound to the current policy label and evaluate the specified policy label.
policyname	<String>	Read-write	Name of the bot policy.
invoke_labelname	<String>	Read-write	* If labelType is policylabel, name of the policy label to invoke. * If labelType is vserver, name of the virtual server.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/botpolicylabel_botpolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"botpolicylabel_botpolicy_binding":{

<b>"labelname":<String_value>,

</b><b>"policyname":<String_value>,

</b><b>"priority":<Integer_value>,

</b>"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>,
```

```
"labeltype":<String_value>,

"invoke_labelname":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/botpolicylabel_botpolicy_binding/ labelname_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ botpolicylabel_botpolicy_binding/ labelname_value<String> ? **args= policyname:<String_value>, priority: <Integer_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/botpolicylabel_botpolicy_binding/ labelname_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ botpolicylabel_botpolicy_binding/ labelname_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of botpolicylabel_botpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/botpolicylabel_botpolicy_binding/ labelname_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the botpolicylabel_botpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "botpolicylabel_botpolicy_binding": [ {

"labelname":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>,

"policyname":<String_value>,

"invoke_labelname":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/botpolicylabel_botpolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/botpolicylabel_botpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "botpolicylabel_botpolicy_binding": [ {

"labelname":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>,

"policyname":<String_value>,

"invoke_labelname":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/botpolicylabel_botpolicy_binding/ labelname_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"botpolicylabel_botpolicy_binding": [ { "__count": "#no"} ] }
```

botpolicylabel_policybinding_binding

Binding object showing the policybinding that can be bound to botpolicylabel.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
labelname	<String>	Read-write	Name of the bot policy label to which to bind the policy.
labeltype	<String>	Read-write	Type of policy label to invoke. Available settings function as follows: * vserver - Invoke an unnamed policy label

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			associated with a virtual server. * policylabel - Invoke a user-defined policy label. Possible values = vserver, policylabel
priority	<Integer>	Read-write	Specifies the priority of the policy.
invoke_labelname	<String>	Read-write	* If labelType is policylabel, name of the policy label to invoke. * If labelType is vserver, name of the virtual server.
gotopriorityexpression	<String>	Read-write	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
invoke	<Boolean>	Read-write	If the current policy evaluates to TRUE, terminate evaluation of policies bound to the current policy label and evaluate the specified policy label.
policyname	<String>	Read-write	Name of the bot policy.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/botpolicylabel_policybinding_binding/ labelname_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ botpolicylabel_policybinding_binding/ labelname_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of botpolicylabel_policybinding_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/botpolicylabel_policybinding_binding/ labelname_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the botpolicylabel_policybinding_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "botpolicylabel_policybinding_binding": [ {

"labelname":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"invoke_labelname":<String_value>,

"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>,

"policyname":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/botpolicylabel_policybinding_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/botpolicylabel_policybinding_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "botpolicylabel_policybinding_binding": [ {

"labelname":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"invoke_labelname":<String_value>,

"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>,
```

```
"policyname":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/botpolicylabel_policybinding_binding/ labelname_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"botpolicylabel_policybinding_binding": [ { "__count": "#no"} ] }
```

botprofile

Configuration for Bot profile resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the profile. Must begin with a letter, number, or the underscore character

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			(_), and must contain only letters, numbers, and the hyphen (-), period (.), pound (#), space ( ), at (@), equals (=), colon (:), and underscore (_) characters. Cannot be changed after the profile is added. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my profile" or 'my profile'). Minimum length = 1 Maximum length = 31
signature	<String>	Read-write	Name of object containing bot static signature details. Minimum length = 1
errorurl	<String>	Read-write	URL that Bot protection uses as the Error URL. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
trapurl	<String>	Read-write	URL that Bot protection uses as the Trap URL. Minimum length = 1 Maximum length = 127
comment	<String>	Read-write	Any comments about the purpose of profile, or other useful information about the profile. Minimum length = 1
bot_enable_white_list	<String>	Read-write	Enable white-list bot detection. Default value: OFF Possible values = ON, OFF
bot_enable_black_list	<String>	Read-write	Enable black-list bot detection. Default value: OFF Possible values = ON, OFF
bot_enable_rate_limit	<String>	Read-write	Enable rate-limit bot detection. Default value: OFF Possible values = ON, OFF
devicefingerprint	<String>	Read-write	Enable device-fingerprint bot detection.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: OFF Possible values = ON, OFF
devicefingerprintaction	<String[]>	Read-write	Action to be taken for device-fingerprint based bot detection. Default value: NONE Possible values = NONE, LOG, DROP, REDIRECT, RESET, MITIGATION
bot_enable_ip_reputation	<String>	Read-write	Enable IP-reputation bot detection. Default value: OFF Possible values = ON, OFF
trap	<String>	Read-write	Enable trap bot detection. Default value: OFF Possible values = ON, OFF
trapaction	<String[]>	Read-write	Action to be taken for bot trap based bot detection. Default value: NONE Possible values = NONE, LOG,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			DROP, REDIRECT, RESET
signaturenouseragentheaderaction	<String[]>	Read-write	Actions to be taken if no User-Agent header in the request (Applicable if Signature check is enabled). Default value: DROP Possible values = NONE, LOG, DROP, REDIRECT, RESET
signaturemultipleuseragentheaderaction	<String[]>	Read-write	Actions to be taken if multiple User-Agent headers are seen in a request (Applicable if Signature check is enabled). Log action should be combined with other actions. Default value: CHECKLAST Possible values = CHECKLAST, LOG, DROP, REDIRECT, RESET
bot_enable_tps	<String>	Read-write	Enable TPS. Default value: OFF Possible values = ON, OFF

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
devicefingerprintmobile	<String[]>	Read-write	Enabling bot device fingerprint protection for mobile clients. Default value: NONE Possible values = NONE, Android, iOS
headlessbrowserdetection	<String>	Read-write	Enable Headless Browser detection. Default value: OFF Possible values = ON, OFF
clientipexpression	<String>	Read-write	Expression to get the client IP.
kmjavascriptname	<String>	Read-write	Name of the JavaScript file that the Bot Management feature will insert in the response for keyboard-mouse based detection. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space ( ), at (@), equals (=), colon (:),

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			and underscore characters. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my javascript file name" or 'my javascript file name').
kmdetection	<String>	Read-write	Enable keyboard-mouse based bot detection. Default value: OFF Possible values = ON, OFF
kmeventspostbodylimit	<Integer>	Read-write	Size of the KM data send by the browser, needs to be processed on ADC. Minimum value = 1 Maximum value = 204800
verboseloglevel	<String>	Read-write	Bot verbose Logging. Based on the log level, ADC will log additional

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			information whenever client is detected as a bot. Default value: NONE Possible values = NONE, HTTP_FULL_HEADER
spoofedreqaction	<String[]>	Read-write	Actions to be taken on a spoofed request (A request spoofing good bot user agent string). Default value: BOT_ACTION_LOG_DROP Possible values = NONE, LOG, DROP, REDIRECT, RESET
dfprequestlimit	<Integer>	Read-write	Number of requests to allow without bot session cookie if device fingerprint is enabled. Minimum value = 1
sessioncookiename	<String>	Read-write	Name of the SessionCookie that the Bot Management feature uses for tracking. Must begin with a letter or number, and can consist of

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			from 1 to 31 letters, numbers, and the hyphen (-) and underscore (_) symbols. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my cookie name" or 'my cookie name'). Minimum length = 1
sessiontimeout	<Integer>	Read-write	Timeout, in seconds, after which a user session is terminated. Minimum value = 1 Maximum value = 65535
addcookieflags	<String>	Read-write	Add the specified flags to bot session cookies. Available settings function as follows:

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			* None - Do not add flags to cookies. * HTTP Only - Add the HTTP Only flag to cookies, which prevents scripts from accessing cookies. * Secure - Add Secure flag to cookies. * All - Add both HTTPOnly and Secure flags to cookies. Default value: httpOnly Possible values = none, httpOnly, secure, all
builtin	<String[]>	Read-only	Flag to determine if bot profille is built-in or not. Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL
feature	<String>	Read-only	The feature to be checked while applying this config.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- UPDATE
- UNSET
- DELETE
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/botprofile? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"botprofile":{

<b>"name":<String_value>,

</b>"signature":true,

"errorurl":true,

"trapurl":true,

"comment":true,

"bot_enable_white_list":true,

"bot_enable_black_list":true,

"bot_enable_rate_limit":true,

"devicefingerprint":true,

"devicefingerprintaction":true,

"bot_enable_ip_reputation":true,

"trap":true,

"signaturenouseragentheaderaction":true,
```

```
"signaturemultipleuseragentheaderaction":true,

"trapaction":true,

"bot_enable_tps":true,

"devicefingerprintmobile":true,

"headlessbrowserdetection":true,

"clientipexpression":true,

"kmjavascriptname":true,

"kmdetection":true,

"kmeventspostbodylimit":true,

"verboseloglevel":true,

"spoofedreqaction":true,

"dfprequestlimit":true,

"sessioncookiename":true,

"sessiontimeout":true,

"addcookieflags":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/botprofile **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"botprofile":{

<b>"name":<String_value>,

</b>"signature":<String_value>,

"errorurl":<String_value>,

"trapurl":<String_value>,

"comment":<String_value>,

"bot_enable_white_list":<String_value>,

"bot_enable_black_list":<String_value>,

"bot_enable_rate_limit":<String_value>,

"devicefingerprint":<String_value>,

"devicefingerprintaction":<String[]_value>,

"bot_enable_ip_reputation":<String_value>,

"trap":<String_value>,

"signaturenouseragentheaderaction":<String[]_value>,

"signaturemultipleuseragentheaderaction":<String[]_value>,

"trapaction":<String[]_value>,

"bot_enable_tps":<String_value>,

"devicefingerprintmobile":<String[]_value>,

"headlessbrowserdetection":<String_value>,
```

```
"clientipexpression":<String_value>,

"kmjavascriptname":<String_value>,

"kmdetection":<String_value>,

"kmeventspostbodylimit":<Integer_value>,

"verboseloglevel":<String_value>,

"spoofedreqaction":<String[]_value>,

"dfprequestlimit":<Integer_value>,

"sessioncookiename":<String_value>,

"sessiontimeout":<Integer_value>,

"addcookieflags":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/botprofile **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"botprofile":{

<b>"name":<String_value>,
```

```
</b>"signature":<String_value>,

"errorurl":<String_value>,

"trapurl":<String_value>,

"comment":<String_value>,

"bot_enable_white_list":<String_value>,

"bot_enable_black_list":<String_value>,

"bot_enable_rate_limit":<String_value>,

"devicefingerprint":<String_value>,

"devicefingerprintaction":<String[]_value>,

"bot_enable_ip_reputation":<String_value>,

"trap":<String_value>,

"trapaction":<String[]_value>,

"signaturenouseragentheaderaction":<String[]_value>,

"signaturemultipleuseragentheaderaction":<String[]_value>,

"bot_enable_tps":<String_value>,

"devicefingerprintmobile":<String[]_value>,

"headlessbrowserdetection":<String_value>,

"clientipexpression":<String_value>,

"kmjavascriptname":<String_value>,

"kmdetection":<String_value>,

"kmeventspostbodylimit":<Integer_value>,

"verboseloglevel":<String_value>,
```

```
"spoofedreqaction":<String[]_value>,

"dfprequestlimit":<Integer_value>,

"sessioncookiename":<String_value>,

"sessiontimeout":<Integer_value>,

"addcookieflags":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/botprofile/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/botprofile **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/botprofile? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/botprofile? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of botprofile resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/botprofile? **view=summary**

Use this query-parameter to get the summary output of botprofile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/botprofile? **pagesize=#no;pageno=#no**

Use this query-parameter to get the botprofile resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "botprofile": [ {

"name":<String_value>,

"signature":<String_value>,

"errorurl":<String_value>,

"trapurl":<String_value>,

"comment":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,
```

```
"bot_enable_white_list":<String_value>,

"bot_enable_black_list":<String_value>,

"bot_enable_rate_limit":<String_value>,

"devicefingerprint":<String_value>,

"devicefingerprintaction":<String[]_value>,

"bot_enable_ip_reputation":<String_value>,

"trap":<String_value>,

"signaturenouseragentheaderaction":<String[]_value>,

"spoofedreqaction":<String[]_value>,

"signaturemultipleuseragentheaderaction":<String[]_value>,

"trapaction":<String[]_value>,

"bot_enable_tps":<String_value>,

"devicefingerprintmobile":<String[]_value>,

"headlessbrowserdetection":<String_value>,

"clientipexpression":<String_value>,

"kmjavascriptname":<String_value>,

"kmdetection":<String_value>,

"kmeventspostbodylimit":<Integer_value>,

"verboseloglevel":<String_value>,

"dfprequestlimit":<Integer_value>,

"sessioncookiename":<String_value>,

"sessiontimeout":<Integer_value>,
```

```
"addcookieflags":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/botprofile/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/botprofile/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/botprofile/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of botprofile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "botprofile": [ {

"name":<String_value>,

"signature":<String_value>,

"errorurl":<String_value>,

"trapurl":<String_value>,

"comment":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"bot_enable_white_list":<String_value>,

"bot_enable_black_list":<String_value>,

"bot_enable_rate_limit":<String_value>,

"devicefingerprint":<String_value>,

"devicefingerprintaction":<String[]_value>,

"bot_enable_ip_reputation":<String_value>,

"trap":<String_value>,

"signaturenouseragentheaderaction":<String[]_value>,

"spoofedreqaction":<String[]_value>,

"signaturemultipleuseragentheaderaction":<String[]_value>,

"trapaction":<String[]_value>,

"bot_enable_tps":<String_value>,

"devicefingerprintmobile":<String[]_value>,

"headlessbrowserdetection":<String_value>,
```

```
"clientipexpression":<String_value>,

"kmjavascriptname":<String_value>,

"kmdetection":<String_value>,

"kmeventspostbodylimit":<Integer_value>,

"verboseloglevel":<String_value>,

"dfprequestlimit":<Integer_value>,

"sessioncookiename":<String_value>,

"sessiontimeout":<Integer_value>,

"addcookieflags":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/botprofile? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "botprofile": [ { "__count": "#no"} ] }
```

botprofile_binding

Binding object which returns the resources bound to botprofile.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the bot management profile. Minimum length = 1 Maximum length = 31
botprofile_trapinsertionurl_binding	<botprofile_trapinsertionurl_binding[]>	Read-only	trapinsertionurl that can be bound to botprofile.
botprofile_whitelist_binding	<botprofile_whitelist_binding[]>	Read-only	whitelist that can be bound to botprofile.
botprofile_ipreputation_binding	<botprofile_ipreputation_binding[]>	Read-only	ipreputation that can be bound to botprofile.
botprofile_logexpression_binding	<botprofile_logexpression_binding[]>	Read-only	logexpression that can be bound to botprofile.
botprofile_blacklist_binding	<botprofile_blacklist_binding[]>	Read-only	blacklist that can be bound to botprofile.
botprofile_tps_binding	<botprofile_tps_binding[]>	Read-only	tps that can be bound to botprofile.
botprofile_ratelimit_binding	<botprofile_ratelimit_binding[]>	Read-only	ratelimit that can be bound to botprofile.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
botprofile_captcha_binding	<botprofile_captcha_binding[]>	Read-only	captcha that can be bound to botprofile.
botprofile_kmdetectionexpr_binding	<botprofile_kmdetectionexpr_binding[]>	Read-only	kmdetectionexpr that can be bound to botprofile.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/botprofile_binding/ name_value<String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "botprofile_binding": [ {

"name":<String_value>,

"botprofile_ratelimit_binding":<botprofile_ratelimit_binding[]_value>,

"botprofile_whitelist_binding":<botprofile_whitelist_binding[]_value>,

"botprofile_trapinsertionurl_binding":<botprofile_trapinsertionurl_binding
[]_value>,

"botprofile_logexpression_binding":<botprofile_logexpression_binding[]_val
ue>,

"botprofile_kmdetectionexpr_binding":<botprofile_kmdetectionexpr_binding[]
_value>,

"botprofile_blacklist_binding":<botprofile_blacklist_binding[]_value>,

"botprofile_captcha_binding":<botprofile_captcha_binding[]_value>,

"botprofile_tps_binding":<botprofile_tps_binding[]_value>,
```

```
"botprofile_ipreputation_binding":<botprofile_ipreputation_binding[]_value
>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/botprofile_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/botprofile_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "botprofile_binding": [ {

"name":<String_value>,

"botprofile_ratelimit_binding":<botprofile_ratelimit_binding[]_value>,

"botprofile_whitelist_binding":<botprofile_whitelist_binding[]_value>,

"botprofile_trapinsertionurl_binding":<botprofile_trapinsertionurl_binding
[]_value>,
```

```
"botprofile_logexpression_binding":<botprofile_logexpression_binding[]_value>,

"botprofile_kmdetectionexpr_binding":<botprofile_kmdetectionexpr_binding[]_value>,

"botprofile_blacklist_binding":<botprofile_blacklist_binding[]_value>,

"botprofile_captcha_binding":<botprofile_captcha_binding[]_value>,

"botprofile_tps_binding":<botprofile_tps_binding[]_value>,

"botprofile_ipreputation_binding":<botprofile_ipreputation_binding[]_value>

}]}
```

botprofile_blacklist_binding

Binding object showing the blacklist that can be bound to botprofile.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
bot_blacklist_enabled	<String>	Read-write	Enabled or disbaled black-list binding. Default value: OFF Possible values = ON, OFF
bot_blacklist_type	<String>	Read-write	Type of the black-list entry. Possible values = IPv4, SUBNET, IPv6, IPv6_SUBNET, EXPRESSION

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the profile. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.), pound (#), space ( ), at (@), equals (=), colon (:), and underscore (_) characters. Cannot be changed after the profile is added.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my profile" or 'my profile').

Minimum length = 1

Maximum length = 31

Minimum length = 1

Default value: NONE

Possible values = NONE, LOG, DROP, RESET, REDIRECT

Minimum length = 1

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)

- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/botprofile_blacklist_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"botprofile_blacklist_binding":{
```

```
<b>"name":<String_value>,

</b>"bot_blacklist":<Boolean_value>,

"bot_blacklist_type":<String_value>,

"bot_blacklist_value":<String_value>,

"bot_blacklist_action":<String[]_value>,

"bot_blacklist_enabled":<String_value>,

"logmessage":<String_value>,

"bot_bind_comment":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/botprofile_blacklist_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ botprofile_blacklist_binding/ name_value<String> ? **args=bot_blacklist: <Boolean_value> ,bot_blacklist_value: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/botprofile_blacklist_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ botprofile_blacklist_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of botprofile_blacklist_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/botprofile_blacklist_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the botprofile_blacklist_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "botprofile_blacklist_binding": [ {

"bot_blacklist_enabled":<String_value>,

"bot_blacklist_type":<String_value>,

"name":<String_value>,

"logmessage":<String_value>,

"bot_blacklist":<Boolean_value>,
```

```
"bot_blacklist_value":<String_value>,

"bot_blacklist_action":<String[]_value>,

"bot_bind_comment":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/botprofile_blacklist_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/botprofile_blacklist_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "botprofile_blacklist_binding": [ {

"bot_blacklist_enabled":<String_value>,

"bot_blacklist_type":<String_value>,
```

```
"name":<String_value>,

"logmessage":<String_value>,

"bot_blacklist":<Boolean_value>,

"bot_blacklist_value":<String_value>,

"bot_blacklist_action":<String[]_value>,

"bot_bind_comment":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/botprofile_blacklist_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"botprofile_blacklist_binding": [ { "__count": "#no"} ] }
```

botprofile_captcha_binding

Binding object showing the captcha that can be bound to botprofile.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
captcharesource	<Boolean>	Read-write	Captcha action binding. For each URL, only one binding is allowed. To update the values of an existing URL binding, user has to first unbind that binding, and then needs to bind the URL again with new values. Maximum 30 bindings can be configured per profile.
bot_bind_comment	<String>	Read-write	Any comments about this binding. Minimum length = 1
name	<String>	Read-write	Name for the profile. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.), pound (#), space ( ), at (@), equals (=), colon (:), and underscore (_) characters. Cannot be changed after the profile is added.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my profile" or 'my profile').

Minimum length = 1

Maximum length = 31

Minimum length = 1

Minimum length = 1

Default value: 3

Minimum value = 1

Maximum value = 10

Default value: 15

Minimum value = 10

Maximum value = 60

Default value: 300

Minimum value = 60

Maximum value = 900

Default value: 900

Minimum value = 60

Maximum value = 900

Default value: 8000

Minimum value = 10

Maximum value = 30000

Default value: NONE

Possible values = NONE, LOG, DROP, REDIRECT, RESET

Default value: OFF

Possible values = ON, OFF

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/botprofile_captcha_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"botprofile_captcha_binding":{

<b>"name":<String_value>,

</b>"captcharesource":<Boolean_value>,

"bot_captcha_url":<String_value>,

"waittime":<Integer_value>,

"graceperiod":<Integer_value>,

"muteperiod":<Integer_value>,

"requestsizelimit":<Integer_value>,

"retryattempts":<Integer_value>,

"bot_captcha_action":<String[]_value>,

"bot_captcha_enabled":<String_value>,

"logmessage":<String_value>,

"bot_bind_comment":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/botprofile_captcha_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ botprofile_captcha_binding/ name_value<String> ? **args=captcharesource: <Boolean_value> ,bot_captcha_url: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/botprofile_captcha_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ botprofile_captcha_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of botprofile_captcha_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/botprofile_captcha_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the botprofile_captcha_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "botprofile_captcha_binding": [ {

"captcharesource":<Boolean_value>,

"bot_bind_comment":<String_value>,

"name":<String_value>,

"logmessage":<String_value>,

"bot_captcha_url":<String_value>,

"retryattempts":<Integer_value>,

"waittime":<Integer_value>,

"muteperiod":<Integer_value>,

"graceperiod":<Integer_value>,

"requestsizelimit":<Integer_value>,

"bot_captcha_action":<String[]_value>,

"bot_captcha_enabled":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/botprofile_captcha_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ botprofile_captcha_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "botprofile_captcha_binding": [ {

"captcharesource":<Boolean_value>,

"bot_bind_comment":<String_value>,

"name":<String_value>,

"logmessage":<String_value>,

"bot_captcha_url":<String_value>,

"retryattempts":<Integer_value>,

"waittime":<Integer_value>,

"muteperiod":<Integer_value>,

"graceperiod":<Integer_value>,

"requestsizelimit":<Integer_value>,

"bot_captcha_action":<String[]_value>,
```

```
"bot_captcha_enabled":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/botprofile_captcha_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"botprofile_captcha_binding": [ { "__count": "#no"} ] }
```

botprofile_ipreputation_binding

Binding object showing the ipreputation that can be bound to botprofile.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
bot_ipreputation	<Boolean>	Read-write	IP reputation binding. For each category, only one binding is allowed. To update

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			the values of an existing binding, user has to first unbind that binding, and then needs to bind again with the new values.
bot_iprep_action	<String[]>	Read-write	One or more actions to be taken if bot is detected based on this IP Reputation binding. Only LOG action can be combinded with DROP, RESET, REDIRECT or MITIGATION action. Default value: NONE Possible values = NONE, LOG, DROP, REDIRECT, RESET, MITIGATION
bot_iprep_enabled	<String>	Read-write	Enabled or disabled IP-repuation binding. Default value: OFF Possible values = ON, OFF
category	<String>	Read-write	IP Repuation category. Following IP Reuputation categories are allowed: *IP_BASED - This category checks whether

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			client IP is malicious or not. *BOTNET - This category includes Botnet C;C channels, and infected zombie machines controlled by Bot master. *SPAM_SOURCES - This category includes tunneling spam messages through a proxy, anomalous SMTP activities, and forum spam activities. *SCANNERS - This category includes all reconnaissance such as probes, host scan, domain scan, and password brute force attack. *DOS - This category includes DOS, DDOS, anomalous sync flood, and anomalous traffic detection. *REPUTATION - This category denies access from IP addresses currently known to be infected with malware. This category also includes IPs with average low Webroot Reputation Index score. Enabling this category will prevent

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			access from sources identified to contact malware distribution points. *PHISHING - This category includes IP addresses hosting phishing sites and other kinds of fraud activities such as ad click fraud or gaming fraud. *PROXY - This category includes IP addresses providing proxy services. *NETWORK - IPs providing proxy and anonymization services including The Onion Router aka TOR or darknet. *MOBILE_THREATS - This category checks client IP with the list of IPs harmful for mobile devices. *WINDOWS_EXPLOITS - This category includes active IP address offering or distributig malware, shell code, rootkits, worms or viruses. *WEB_ATTACKS - This category includes cross site scripting, iFrame injection, SQL injection, cross domain injection or

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			domain password brute force attack. *TOR_PROXY - This category includes IP address acting as exit nodes for the Tor Network. *CLOUD - This category checks client IP with list of public cloud IPs. *CLOUD_AWS - This category checks client IP with list of public cloud IPs from Amazon Web Services. *CLOUD_GCP - This category checks client IP with list of public cloud IPs from Google Cloud Platform. *CLOUD_AZURE - This category checks client IP with list of public cloud IPs from Azure. *CLOUD_ORACLE - This category checks client IP with list of public cloud IPs from Oracle. *CLOUD_IBM - This category checks client IP with list of public cloud IPs from IBM. *CLOUD_SALESFORCE - This category checks client IP with

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			list of public cloud IPs from Salesforce. Possible values = IP, BOTNETS, SPAM_SOURCES, SCANNERS, DOS, REPUTATION, PHISHING, PROXY, NETWORK, MOBILE_THREATS, WINDOWS_EXPLOITS, WEB_ATTACKS, TOR_PROXY, CLOUD, CLOUD_AWS, CLOUD_GCP, CLOUD_AZURE, CLOUD_ORACLE, CLOUD_IBM, CLOUD_SALESFORCE
bot_bind_comment	<String>	Read-write	Any comments about this binding. Minimum length = 1
logmessage	<String>	Read-write	Message to be logged for this binding. Minimum length = 1
name	<String>	Read-write	Name for the profile. Must begin with a letter, number, or the underscore character

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			(_), and must contain only letters, numbers, and the hyphen (-), period (.), pound (#), space ( ), at (@), equals (=), colon (:), and underscore (_) characters. Cannot be changed after the profile is added.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my profile" or 'my profile').

Minimum length = 1

Maximum length = 31

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/botprofile_ipreputation_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"botprofile_ipreputation_binding":{

<b>"name":<String_value>,

</b>"bot_ipreputation":<Boolean_value>,

"category":<String_value>,

"bot_iprep_enabled":<String_value>,

"bot_iprep_action":<String[]_value>,
```

```
"logmessage":<String_value>,

"bot_bind_comment":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/botprofile_ipreputation_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ botprofile_ipreputation_binding/ name_value<String> ? **args=bot_ipreputation: <Boolean_value> ,category: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/botprofile_ipreputation_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ botprofile_ipreputation_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of botprofile_ipreputation_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/botprofile_ipreputation_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the botprofile_ipreputation_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "botprofile_ipreputation_binding": [ {

"bot_ipreputation":<Boolean_value>,

"bot_iprep_action":<String[]_value>,

"bot_iprep_enabled":<String_value>,

"category":<String_value>,

"bot_bind_comment":<String_value>,

"logmessage":<String_value>,

"name":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/botprofile_ipreputation_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ botprofile_ipreputation_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "botprofile_ipreputation_binding": [ {

"bot_ipreputation":<Boolean_value>,

"bot_iprep_action":<String[]_value>,

"bot_iprep_enabled":<String_value>,

"category":<String_value>,

"bot_bind_comment":<String_value>,

"logmessage":<String_value>,

"name":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/botprofile_ipreputation_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"botprofile_ipreputation_binding": [ { "__count": "#no"} ] }
```

botprofile_kmdetectionexpr_binding

Binding object showing the kmdetectionexpr that can be bound to botprofile.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
logmessage	<String>	Read-write	Message to be logged for this binding. Minimum length = 1
name	<String>	Read-write	Name for the profile. Must begin with a letter, number, or the underscore character (_), and must contain

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			only letters, numbers, and the hyphen (-), period (.), pound (#), space ( ), at (@), equals (=), colon (:), and underscore (_) characters. Cannot be changed after the profile is added.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my profile" or 'my profile').

Minimum length = 1

Maximum length = 31

Minimum length = 1

Minimum length = 1

Default value: OFF

Possible values = ON, OFF

Minimum length = 1

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/botprofile_kmdetectionexpr_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"botprofile_kmdetectionexpr_binding":{

<b>"name":<String_value>,
```

```
</b>"kmdetectionexpr":<Boolean_value>,

"bot_km_expression_name":<String_value>,

"bot_km_expression_value":<String_value>,

"bot_km_detection_enabled":<String_value>,

"logmessage":<String_value>,

"bot_bind_comment":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/botprofile_kmdetectionexpr_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ botprofile_kmdetectionexpr_binding/ name_value<String> ? **args=kmdetectionexpr: <Boolean_value> ,bot_km_expression_name: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/botprofile_kmdetectionexpr_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/

botprofile_kmdetectionexpr_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of botprofile_kmdetectionexpr_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/botprofile_kmdetectionexpr_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the botprofile_kmdetectionexpr_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "botprofile_kmdetectionexpr_binding": [ {

"logmessage":<String_value>,

"name":<String_value>,

"bot_km_expression_value":<String_value>,

"bot_bind_comment":<String_value>,

"bot_km_detection_enabled":<String_value>,

"kmdetectionexpr":<Boolean_value>,
```

```
"bot_km_expression_name":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/botprofile_kmdetectionexpr_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/botprofile_kmdetectionexpr_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "botprofile_kmdetectionexpr_binding": [ {

"logmessage":<String_value>,

"name":<String_value>,

"bot_km_expression_value":<String_value>,

"bot_bind_comment":<String_value>,
```

```
"bot_km_detection_enabled":<String_value>,

"kmdetectionexpr":<Boolean_value>,

"bot_km_expression_name":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/botprofile_kmdetectionexpr_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"botprofile_kmdetectionexpr_binding": [ { "__count": "#no"} ] }
```

botprofile_logexpression_binding

Binding object showing the logexpression that can be bound to botprofile.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
logexpression	<Boolean>	Read-write	Log expression binding.
bot_log_expression_value	<String>	Read-write	Expression whose result to be logged when violation happened on the bot profile. Minimum length = 1
bot_log_expression_enabled	<String>	Read-write	Enable or disable the log expression binding. Default value: OFF Possible values = ON, OFF
bot_log_expression_name	<String>	Read-write	Name of the log expression object. Minimum length = 1
bot_bind_comment	<String>	Read-write	Any comments about this binding. Minimum length = 1
name	<String>	Read-write	Name for the profile. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.), pound (#), space ( ), at (@), equals (=), colon (:), and underscore (_) characters. Cannot

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			be changed after the profile is added.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my profile" or 'my profile').

Minimum length = 1

Maximum length = 31

Minimum length = 1

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/botprofile_logexpression_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"botprofile_logexpression_binding":{

<b>"name":<String_value>,

</b>"logexpression":<Boolean_value>,

"bot_log_expression_name":<String_value>,

"bot_log_expression_value":<String_value>,

"bot_log_expression_enabled":<String_value>,

"logmessage":<String_value>,

"bot_bind_comment":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/botprofile_logexpression_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ botprofile_logexpression_binding/ name_value<String> ? **args=logexpression: <Boolean_value> ,bot_log_expression_name: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/botprofile_logexpression_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ botprofile_logexpression_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of botprofile_logexpression_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/botprofile_logexpression_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the botprofile_logexpression_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "botprofile_logexpression_binding": [ {

"logexpression":<Boolean_value>,

"bot_log_expression_value":<String_value>,

"bot_log_expression_enabled":<String_value>,

"bot_log_expression_name":<String_value>,

"bot_bind_comment":<String_value>,

"name":<String_value>,

"logmessage":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/botprofile_logexpression_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/botprofile_logexpression_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "botprofile_logexpression_binding": [ {

"logexpression":<Boolean_value>,

"bot_log_expression_value":<String_value>,

"bot_log_expression_enabled":<String_value>,

"bot_log_expression_name":<String_value>,

"bot_bind_comment":<String_value>,

"name":<String_value>,

"logmessage":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/botprofile_logexpression_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"botprofile_logexpression_binding": [ { "__count": "#no"} ] }
```

botprofile_ratelimit_binding

Binding object showing the ratelimit that can be bound to botprofile.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
limittype	<String>	Read-write	Rate-Limiting traffic Type. Default value: BURSTY Possible values = BURSTY, SMOOTH
bot_rate_limit_type	<String>	Read-write	Rate-limiting type Following rate-limiting types are allowed: *SOURCE_IP - Rate-limiting based on the client IP. *SESSION - Rate-limiting based on the configured cookie name. *URL - Rate-limiting based on the configured URL. *GEOLOCATION -

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Rate-limiting based on the configured country name. *JA3_FINGERPRINT - Rate-limiting based on client SSL JA3 fingerprint. Possible values = SESSION, SOURCE_IP, URL, GEOLOCATION, JA3_FINGERPRINT
timeslice	<Integer>	Read-write	Time interval during which requests are tracked to check if they cross the given rate. Default value: 1000 Minimum value = 10
condition	<String>	Read-write	Expression to be used in a rate-limiting condition. This expression result must be a boolean value.
countrycode	<String>	Read-write	Country name which is used for geolocation rate-limiting. Possible values = AF, AX, AL, DZ, AS, AD, AO, AI, AQ, AG, AR, AM, AW, AU, AT, AZ, BS, BH, BD, BB, BY, BE, BZ, BJ,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			BM, BT, BO, BQ, BA, BW, BR, IO, BN, BG, BF, BI, KH, CM, CA, CV, KY, CF, TD, CL, CN, CX, CC, CO, KM, CG, CD, CK, CR, CI, HR, CU, CW, CY, CZ, DK, DJ, DM, DO, EC, EG, SV, GQ, ER, EE, ET, FK, FO, FJ, FI, FR, GF, PF, TF, GA, GM, GE, DE, GH, GI, GR, GL, GD, GP, GU, GT, GG, GN, GW, GY, HT, HM, VA, HN, HK, HU, IS, IN, ID, IR, IQ, IE, IM, IL, IT, JM, JP, JE, JO, KZ, KE, KI, XK, KW, KG, LA, LV, LB, LS, LR, LY, LI, LT, LU, MO, MK, MG, MW, MY, MV, ML, MT, MH, MQ, MR, MU, YT, MX, FM, MD, MC, MN, ME, MS, MA, MZ, MM, NA, NR, NP, NL, NC, NZ, NI, NE, NG, NU, NF, KP, MP, NO, OM, PK, PW, PS, PA, PG, PY, PE, PH, PN, PL, PT,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			PR, QA, RE, RO, RU, RW, BL, SH, KN, LC, MF, PM, VC, WS, SM, ST, SA, SN, RS, SC, SL, SG, SX, SK, SI, SB, SO, SZA, GS, KR, SS, ES, LK, SD, SR, SJ, SZ, SE, CH, SY, TW, TJ, TZ, TH, TL, TG, TK, TO, TT, TN, TR, TM, TC, TV, UG, UA, AE, GB, US, UM, UY, UZ, VU, VE, VN, VG, VI, WF, EH, YE, ZM, ZW
bot_rate_limit_url	<String>	Read-write	URL for the resource based rate-limiting.
cookiename	<String>	Read-write	Cookie name which is used to identify the session for session rate-limiting.
name	<String>	Read-write	Name for the profile. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.), pound (#), space ( ), at (@), equals (=), colon (:), and underscore (_)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			characters. Cannot be changed after the profile is added.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my profile" or 'my profile').

Minimum length = 1

Maximum length = 31

Minimum length = 1

Default value: NONE

Possible values = NONE, LOG, DROP, REDIRECT, RESET, RESPOND_STATUS_TOO_MANY_REQUESTS

Minimum length = 1

Default value: OFF

Possible values = ON, OFF

Default value: 1

Minimum value = 1

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/botprofile_ratelimit_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"botprofile_ratelimit_binding":{

<b>"name":<String_value>,

</b>"bot_ratelimit":<Boolean_value>,
```

```
"bot_rate_limit_type":<String_value>,

"bot_rate_limit_url":<String_value>,

"cookiename":<String_value>,

"countrycode":<String_value>,

"rate":<Integer_value>,

"timeslice":<Integer_value>,

"limittype":<String_value>,

"condition":<String_value>,

"bot_rate_limit_action":<String[]_value>,

"bot_rate_limit_enabled":<String_value>,

"logmessage":<String_value>,

"bot_bind_comment":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/botprofile_ratelimit_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ botprofile_ratelimit_binding/ name_value<String> ? **args=bot_ratelimit: <Boolean_value> ,bot_rate_limit_type: <String_value> ,bot_rate_limit_url: <String_value> ,cookiename: <String_value> ,countrycode: <String_value> ,condition: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/botprofile_ratelimit_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ botprofile_ratelimit_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of botprofile_ratelimit_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/botprofile_ratelimit_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the botprofile_ratelimit_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "botprofile_ratelimit_binding": [ {

"limittype":<String_value>,

"bot_rate_limit_type":<String_value>,

"timeslice":<Integer_value>,

"condition":<String_value>,

"countrycode":<String_value>,

"bot_rate_limit_url":<String_value>,

"cookiename":<String_value>,

"name":<String_value>,

"logmessage":<String_value>,

"bot_rate_limit_action":<String[]_value>,

"bot_ratelimit":<Boolean_value>,

"bot_bind_comment":<String_value>,

"bot_rate_limit_enabled":<String_value>,

"rate":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/botprofile_ratelimit_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ botprofile_ratelimit_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "botprofile_ratelimit_binding": [ {

"limittype":<String_value>,

"bot_rate_limit_type":<String_value>,

"timeslice":<Integer_value>,

"condition":<String_value>,

"countrycode":<String_value>,

"bot_rate_limit_url":<String_value>,

"cookiename":<String_value>,

"name":<String_value>,

"logmessage":<String_value>,

"bot_rate_limit_action":<String[]_value>,

"bot_ratelimit":<Boolean_value>,

"bot_bind_comment":<String_value>,
```

```
"bot_rate_limit_enabled":<String_value>,

"rate":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/botprofile_ratelimit_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"botprofile_ratelimit_binding": [ { "__count": "#no"} ] }
```

botprofile_tps_binding

Binding object showing the tps that can be bound to botprofile.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
bot_tps	<Boolean>	Read-write	TPS binding. For each type only

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			binding can be configured. To update the values of an existing binding, user has to first unbind that binding, and then needs to bind again with new values.
bot_tps_type	<String>	Read-write	Type of TPS binding. Possible values = SOURCE_IP, GEOLOCATION, REQUEST_URL, Host
percentage	<Integer>	Read-write	Maximum percentage increase in the requests from (or to) a IP, Geolocation, URL or Host in 30 minutes interval. Minimum value = 10
bot_tps_enabled	<String>	Read-write	Enabled or disabled TPS binding. Default value: ON Possible values = ON, OFF
bot_bind_comment	<String>	Read-write	Any comments about this binding. Minimum length = 1
threshold	<Integer>	Read-write	Maximum number of requests that are allowed from (or to) a

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			IP, Geolocation, URL or Host in 1 second time interval. Minimum value = 1
bot_tps_action	<String[]>	Read-write	One to more actions to be taken if bot is detected based on this TPS binding. Only LOG action can be combined with DROP, RESET, REDIRECT, or MITIGATION action. Default value: NONE Possible values = NONE, LOG, DROP, REDIRECT, RESET, MITIGATION
logmessage	<String>	Read-write	Message to be logged for this binding. Minimum length = 1
name	<String>	Read-write	Name for the profile. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.), pound (#), space ( ), at (@), equals (=), colon (:), and underscore (_)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			characters. Cannot be changed after the profile is added.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my profile" or 'my profile').

Minimum length = 1

Maximum length = 31

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/botprofile_tps_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"botprofile_tps_binding":{

<b>"name":<String_value>,

</b>"bot_tps":<Boolean_value>,

"bot_tps_type":<String_value>,

"threshold":<Integer_value>,

"percentage":<Integer_value>,

"bot_tps_action":<String[]_value>,

"bot_tps_enabled":<String_value>,

"logmessage":<String_value>,

"bot_bind_comment":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/botprofile_tps_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/botprofile_tps_binding/ name_value<String> ? **args=bot_tps: <Boolean_value> ,bot_tps_type: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/botprofile_tps_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/botprofile_tps_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of botprofile_tps_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/botprofile_tps_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the botprofile_tps_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "botprofile_tps_binding": [ {

"bot_tps":<Boolean_value>,

"bot_tps_type":<String_value>,

"percentage":<Integer_value>,

"bot_tps_enabled":<String_value>,

"bot_bind_comment":<String_value>,

"threshold":<Integer_value>,

"bot_tps_action":<String[]_value>,

"logmessage":<String_value>,

"name":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/botprofile_tps_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/botprofile_tps_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "botprofile_tps_binding": [ {

"bot_tps":<Boolean_value>,

"bot_tps_type":<String_value>,

"percentage":<Integer_value>,

"bot_tps_enabled":<String_value>,

"bot_bind_comment":<String_value>,

"threshold":<Integer_value>,

"bot_tps_action":<String[]_value>,

"logmessage":<String_value>,

"name":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/botprofile_tps_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"botprofile_tps_binding": [ { "__count": "#no"} ] }
```

botprofile_trapinsertionurl_binding

Binding object showing the trapinsertionurl that can be bound to botprofile.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
trapinsertionurl	<Boolean>	Read-write	Bind the trap URL for the configured request URLs. Maximum 30 bindings can be configured per profile.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
bot_trap_url	<String>	Read-write	Request URL regex pattern for which Trap URL is inserted. Minimum length = 1
bot_trap_url_insertion_enabled	<String>	Read-write	Enable or disable the request URL pattern. Default value: OFF Possible values = ON, OFF
name	<String>	Read-write	Name for the profile. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.), pound (#), space ( ), at (@), equals (=), colon (:), and underscore (_) characters. Cannot be changed after the profile is added.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my profile" or 'my profile').

Minimum length = 1

Maximum length = 31

Minimum length = 1

Minimum length = 1

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/botprofile_trapinsertionurl_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"botprofile_trapinsertionurl_binding":{

<b>"name":<String_value>,

</b>"trapinsertionurl":<Boolean_value>,

"bot_trap_url":<String_value>,

"bot_trap_url_insertion_enabled":<String_value>,

"logmessage":<String_value>,

"bot_bind_comment":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/botprofile_trapinsertionurl_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ botprofile_trapinsertionurl_binding/ name_value<String> ? **args=trapinsertionurl: <Boolean_value> ,bot_trap_url: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/botprofile_trapinsertionurl_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ botprofile_trapinsertionurl_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of botprofile_trapinsertionurl_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/botprofile_trapinsertionurl_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the botprofile_trapinsertionurl_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "botprofile_trapinsertionurl_binding": [ {

"trapinsertionurl":<Boolean_value>,

"bot_trap_url":<String_value>,

"bot_trap_url_insertion_enabled":<String_value>,
```

```
"name":<String_value>,

"logmessage":<String_value>,

"bot_bind_comment":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/botprofile_trapinsertionurl_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/botprofile_trapinsertionurl_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "botprofile_trapinsertionurl_binding": [ {

"trapinsertionurl":<Boolean_value>,

"bot_trap_url":<String_value>,
```

```
"bot_trap_url_insertion_enabled":<String_value>,

"name":<String_value>,

"logmessage":<String_value>,

"bot_bind_comment":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/botprofile_trapinsertionurl_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"botprofile_trapinsertionurl_binding": [ { "__count": "#no"} ] }
```

botprofile_whitelist_binding

Binding object showing the whitelist that can be bound to botprofile.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
log	<String>	Read-write	Enable logging for Whitelist binding. Default value: OFF Possible values = ON, OFF
name	<String>	Read-write	Name for the profile. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.), pound (#), space ( ), at (@), equals (=), colon (:), and underscore (_) characters. Cannot be changed after the profile is added.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my profile" or 'my profile').

Minimum length = 1

Maximum length = 31

Minimum length = 1

Minimum length = 1

Default value: OFF

Possible values = ON, OFF

Possible values = IPv4, SUBNET, IPv6, IPv6_SUBNET, EXPRESSION

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/botprofile_whitelist_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"botprofile_whitelist_binding":{

<b>"name":<String_value>,

</b>"bot_whitelist":<Boolean_value>,

"bot_whitelist_type":<String_value>,

"bot_whitelist_value":<String_value>,

"log":<String_value>,

"bot_whitelist_enabled":<String_value>,

"logmessage":<String_value>,

"bot_bind_comment":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/botprofile_whitelist_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ botprofile_whitelist_binding/ name_value<String> ? **args=bot_whitelist: <Boolean_value> ,bot_whitelist_value: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/botprofile_whitelist_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ botprofile_whitelist_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of botprofile_whitelist_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/botprofile_whitelist_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the botprofile_whitelist_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "botprofile_whitelist_binding": [ {

"log":<String_value>,
```

```
"name":<String_value>,

"logmessage":<String_value>,

"bot_bind_comment":<String_value>,

"bot_whitelist":<Boolean_value>,

"bot_whitelist_value":<String_value>,

"bot_whitelist_enabled":<String_value>,

"bot_whitelist_type":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/botprofile_whitelist_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/botprofile_whitelist_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "botprofile_whitelist_binding": [ {

"log":<String_value>,

"name":<String_value>,

"logmessage":<String_value>,

"bot_bind_comment":<String_value>,

"bot_whitelist":<Boolean_value>,

"bot_whitelist_value":<String_value>,

"bot_whitelist_enabled":<String_value>,

"bot_whitelist_type":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/botprofile_whitelist_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"botprofile_whitelist_binding": [ { "__count": "#no"} ] }
```

botsettings

Configuration for Bot engine settings resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
defaultprofile	<String>	Read-write	Profile to use when a connection does not match any policy. Default setting is " ", which sends unmatched connections back to the Citrix ADC without attempting to filter them further. Minimum length = 1
defaultnonintrusiveprofile	<String>	Read-write	Profile to use when the feature is not enabled but feature is licensed. NonIntrusive checks will be disabled and IPRep cronjob(24 Hours) will be removed if this is set to BOT_BYPASS. Default value: BOT_STATS Minimum length = 1 Possible values = BOT_BYPASS,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			BOT_STATS, BOT_LOG
javascriptname	<String>	Read-write	Name of the JavaScript that the Bot Management feature uses in response. Must begin with a letter or number, and can consist of from 1 to 31 letters, numbers, and the hyphen (-) and underscore (_) symbols. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my cookie name" or 'my cookie name'). Minimum length = 1
sessiontimeout	<Integer>	Read-write	Timeout, in seconds, after which a user session is terminated.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum value = 1 Maximum value = 65535
sessioncookiename	<String>	Read-write	Name of the SessionCookie that the Bot Management feature uses for tracking. Must begin with a letter or number, and can consist of from 1 to 31 letters, numbers, and the hyphen (-) and underscore (_) symbols. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my cookie name" or 'my cookie name'). Minimum length = 1
dfprequestlimit	<Integer>	Read-write	Number of requests to allow without bot session cookie if

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			device fingerprint is enabled. Minimum value = 1
signatureautoupdate	<String>	Read-write	Flag used to enable/disable bot auto update signatures. Default value: OFF Possible values = ON, OFF
signatureurl	<String>	Read-write	URL to download the bot signature mapping file from server. Default value: https://nsbotsignatures.s3.amazonaws.com/BotSignatureMapping.json
proxyserver	<String>	Read-write	Proxy Server IP to get updated signatures from AWS.
proxyport	<Integer>	Read-write	Proxy Server Port to get updated signatures from AWS. Default value: 8080 Range 1 - 65535 * in CLI is represented as 65535 in NITRO API

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
trapurlautogenerate	<String>	Read-write	Enable/disable trap URL auto generation. When enabled, trap URL is updated within the configured interval. Default value: OFF Possible values = ON, OFF
trapurlinterval	<Integer>	Read-write	Time in seconds after which trap URL is updated. Default value: 3600 Minimum value = 300 Maximum value = 86400
trapurllength	<Integer>	Read-write	Length of the auto-generated trap URL. Default value: 32 Minimum value = 10 Maximum value = 255
proxyusername	<String>	Read-write	Proxy Username. Minimum length = 1
proxypassword	<String>	Read-write	Password with which user logs on. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
builtin	<String[]>	Read-only	Flag to determine if bot engine setting is built-in or not. Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL
feature	<String>	Read-only	The feature to be checked while applying this config.
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- UPDATE
- UNSET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.
- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/botsettings **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"botsettings":{

"defaultprofile":<String_value>,

"defaultnonintrusiveprofile":<String_value>,

"javascriptname":<String_value>,

"sessiontimeout":<Integer_value>,

"sessioncookiename":<String_value>,

"dfprequestlimit":<Integer_value>,

"signatureautoupdate":<String_value>,

"signatureurl":<String_value>,

"proxyserver":<String_value>,

"proxyport":<Integer_value>,
```

```
"trapurlautogenerate":<String_value>,

"trapurlinterval":<Integer_value>,

"trapurllength":<Integer_value>,

"proxyusername":<String_value>,

"proxypassword":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/botsettings? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"botsettings":{

"defaultprofile":true,

"defaultnonintrusiveprofile":true,

"javascriptname":true,

"sessiontimeout":true,

"sessioncookiename":true,
```

```
"dfprequestlimit":true,

"signatureautoupdate":true,

"signatureurl":true,

"proxyserver":true,

"proxyport":true,

"trapurlautogenerate":true,

"trapurlinterval":true,

"trapurllength":true,

"proxyusername":true,

"proxypassword":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/botsettings **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "botsettings": [ {

"defaultprofile":<String_value>,

"defaultnonintrusiveprofile":<String_value>,

"javascriptname":<String_value>,

"sessiontimeout":<Integer_value>,

"sessioncookiename":<String_value>,

"dfprequestlimit":<Integer_value>,

"signatureautoupdate":<String_value>,

"signatureurl":<String_value>,

"proxyserver":<String_value>,

"proxyport":<Integer_value>,

"proxyusername":<String_value>,

"proxypassword":<String_value>,

"trapurlautogenerate":<String_value>,

"trapurlinterval":<Integer_value>,

"trapurllength":<Integer_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

botsignature

Configuration for bot signatures resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
src	<String>	Read-write	Local path to and name of, or URL (protocol, host, path, and file name) for, the file in which to store the imported signature file. NOTE: The import fails if the object to be imported is on an HTTPS server that requires client certificate authentication for access. Minimum length = 1 Maximum length = 2047
name	<String>	Read-write	Name to assign to the bot signature file object on the Citrix ADC. Minimum length = 1 Maximum length = 31

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
comment	<String>	Read-write	Any comments to preserve information about the signature file object. Maximum length = 128
overwrite	<Boolean>	Read-write	Overwrites the existing file.
response	<String>	Read-only	.
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- IMPORT
- DELETE
- CHANGE
- GET (ALL)
- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

IMPORT

URL: http:// <netscaler-ip-address> /nitro/v1/config/botsignature? **action=Import HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"botsignature":{

"src":<String_value>,

<b>"name":<String_value>,

</b>"comment":<String_value>,

"overwrite":<Boolean_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/botsignature/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

CHANGE

URL: http:// <netscaler-ip-address> /nitro/v1/config/botsignature? **action=update HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"botsignature":{

<b>"name":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/botsignature **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "botsignature": [ {

"name":<String_value>,

"response":<String_value>,

"src":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/botsignature/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/botsignature/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/botsignature/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of botsignature resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "botsignature": [ {

"name":<String_value>,

"response":<String_value>,

"src":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

cache

Integrated Caching

Integrated Caching Configuration. The Integrated Caching feature is used to cache static and dynamic web application data.

NAME	DESCRIPTION
cachecontentgroup	Configuration for Integrated Cache content group

NAME	DESCRIPTION
cacheforwardproxy	Configuration for forward proxy
cacheglobal_binding	Binding object showing the resources that can be bound to cacheglobal
cacheglobal_cachepolicy_binding	Binding object showing the cachepolicy that can be bound to cacheglobal
cacheobject	Configuration for cache object
cacheparameter	Configuration for cache parameter
cachepolicy	Configuration for Integrated Cache policy
cachepolicy_binding	Binding object showing the resources that can be bound to cachepolicy
cachepolicy_cacheglobal_binding	Binding object showing the cacheglobal that can be bound to cachepolicy
cachepolicy_cachepolicylabel_binding	Binding object showing the cachepolicylabel that can be bound to cachepolicy
cachepolicy_csvserver_binding	Binding object showing the csvserver that can be bound to cachepolicy
cachepolicy_lbvserver_binding	Binding object showing the lbvserver that can be bound to cachepolicy
cachepolicylabel	Configuration for cache policy label

NAME	DESCRIPTION
cachepolicylabel_binding	Binding object showing the resources that can be bound to cachepolicylabel
cachepolicylabel_cachepolicy_binding	Binding object showing the cachepolicy that can be bound to cachepolicylabel
cachepolicylabel_policybinding_binding	Binding object showing the policybinding that can be bound to cachepolicylabel
cacheselector	Configuration for cache selector

cachecontentgroup

Configuration for Integrated Cache content group resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the content group. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the content group is created.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum length = 1
weakposrelexpiry	<Integer>	Read-write	Relative expiry time, in seconds, for expiring positive responses with response codes between 200 and 399. Cannot be used in combination with other Expiry attributes. Similar to -relExpiry but has lower precedence. Minimum value = 0 Maximum value = 31536000
heurexpiryparam	<Integer>	Read-write	Heuristic expiry time, in percent of the duration, since the object was last modified. Minimum value = 0 Maximum value = 100
relexpiry	<Integer>	Read-write	Relative expiry time, in seconds, after which to expire an object cached in this content group. Minimum value = 0 Maximum value = 31536000
relexpirymillisec	<Integer>	Read-write	Relative expiry time, in milliseconds, after

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			which to expire an object cached in this content group. Minimum value = 0 Maximum value = 86400000
absexpiry	<String[]>	Read-write	Local time, up to 4 times a day, at which all objects in the content group must expire. CLI Users: For example, to specify that the objects in the content group should expire by 11:00 PM, type the following command: add cache contentgroup <contentgroup name> -absexpiry 23:00 To specify that the objects in the content group should expire at 10:00 AM, 3 PM, 6 PM, and 11:00 PM, type: add cache contentgroup <contentgroup name> -absexpiry

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			10:00 15:00 18:00 23:00.
absexpirygmt	<String[]>	Read-write	Coordinated Universal Time (GMT), up to 4 times a day, when all objects in the content group must expire.
weaknegrelexpiry	<Integer>	Read-write	Relative expiry time, in seconds, for expiring negative responses. This value is used only if the expiry time cannot be determined from any other source. It is applicable only to the following status codes: 307, 403, 404, and 410. Minimum value = 0 Maximum value = 31536000
hitparams	<String[]>	Read-write	Parameters to use for parameterized hit evaluation of an object. Up to 128 parameters can be specified. Mutually exclusive with the Hit Selector parameter. Minimum length = 1
invalparams	<String[]>	Read-write	Parameters for parameterized invalidation of an

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			object. You can specify up to 8 parameters. Mutually exclusive with invalSelector. Minimum length = 1
ignoreparamvaluecase	<String>	Read-write	Ignore case when comparing parameter values during parameterized hit evaluation. (Parameter value case is ignored by default during parameterized invalidation.). Possible values = YES, NO
matchcookies	<String>	Read-write	Evaluate for parameters in the cookie header also. Possible values = YES, NO
invalrestrictedtohost	<String>	Read-write	Take the host header into account during parameterized invalidation. Possible values = YES, NO
polleverytime	<String>	Read-write	Always poll for the objects in this content group. That is, retrieve the objects from the origin server

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			whenever they are requested. Default value: NO Possible values = YES, NO
ignorereloadreq	<String>	Read-write	Ignore any request to reload a cached object from the origin server. To guard against Denial of Service attacks, set this parameter to YES. For RFC-compliant behavior, set it to NO. Default value: YES Possible values = YES, NO
removecookies	<String>	Read-write	Remove cookies from responses. Default value: YES Possible values = YES, NO
prefetch	<String>	Read-write	Attempt to refresh objects that are about to go stale. Default value: YES Possible values = YES, NO

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
prefetchperiod	<Integer>	Read-write	Time period, in seconds before an object's calculated expiry time, during which to attempt prefetch. Minimum value = 0 Maximum value = 4294967294
prefetchperiodmillisec	<Integer>	Read-write	Time period, in milliseconds before an object's calculated expiry time, during which to attempt prefetch. Minimum value = 0 Maximum value = 4294967290
prefetchmaxpending	<Integer>	Read-write	Maximum number of outstanding prefetches that can be queued for the content group. Minimum value = 0 Maximum value = 4294967294
flashcache	<String>	Read-write	Perform flash cache. Mutually exclusive with Poll Every Time (PET) on the same content group. Default value: NO

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = YES, NO
expireatlastbyte	<String>	Read-write	Force expiration of the content immediately after the response is downloaded (upon receipt of the last byte of the response body). Applicable only to positive responses. Default value: NO Possible values = YES, NO
insertvia	<String>	Read-write	Insert a Via header into the response. Default value: YES Possible values = YES, NO
insertage	<String>	Read-write	Insert an Age header into the response. An Age header contains information about the age of the object, in seconds, as calculated by the integrated cache. Default value: YES Possible values = YES, NO
insertetag	<String>	Read-write	Insert an ETag header in the response. With ETag

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			header insertion, the integrated cache does not serve full responses on repeat requests. Default value: YES Possible values = YES, NO
cachecontrol	<String>	Read-write	Insert a Cache-Control header into the response. Minimum length = 1
quickabortsize	<Integer>	Read-write	If the size of an object that is being downloaded is less than or equal to the quick abort value, and a client aborts during the download, the cache stops downloading the response. If the object is larger than the quick abort size, the cache continues to download the response. Default value: 4194303 Minimum value = 0 Maximum value = 4194303
minressize	<Integer>	Read-write	Minimum size of a response that can be

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			cached in this content group. Default minimum response size is 0. Minimum value = 0 Maximum value = 2097151
maxressize	<Integer>	Read-write	Maximum size of a response that can be cached in this content group. Default value: 80 Minimum value = 0 Maximum value = 2097151
memlimit	<Integer>	Read-write	Maximum amount of memory that the cache can use. The effective limit is based on the available memory of the Citrix ADC. Default value: 65536
ignorereqcachinghdrs	<String>	Read-write	Ignore Cache-Control and Pragma headers in the incoming request. Default value: YES Possible values = YES, NO

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
minhits	<Integer>	Read-write	Number of hits that qualifies a response for storage in this content group. Default value: 0
alwaysevalpolicies	<String>	Read-write	Force policy evaluation for each response arriving from the origin server. Cannot be set to YES if the Prefetch parameter is also set to YES. Default value: NO Possible values = YES, NO
persistha	<String>	Read-write	Setting persistHA to YES causes IC to save objects in contentgroup to Secondary node in HA deployment. Default value: NO Possible values = YES, NO
pinned	<String>	Read-write	Do not flush objects from this content group under memory pressure. Default value: NO Possible values = YES, NO

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
lazydnsresolve	<String>	Read-write	Perform DNS resolution for responses only if the destination IP address in the request does not match the destination IP address of the cached response. Default value: YES Possible values = YES, NO
hitselector	<String>	Read-write	Selector for evaluating whether an object gets stored in a particular content group. A selector is an abstraction for a collection of PIXL expressions.
invalselector	<String>	Read-write	Selector for invalidating objects in the content group. A selector is an abstraction for a collection of PIXL expressions.
type	<String>	Read-write	The type of the content group. Default value: HTTP Possible values = HTTP, MYSQL, MSSQL

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
query	<String>	Read-write	Query string specifying individual objects to flush from this group by using parameterized invalidation. If this parameter is not set, all objects are flushed from the group. Minimum length = 1
host	<String>	Read-write	Flush only objects that belong to the specified host. Do not use except with parameterized invalidation. Also, the Invalidation Restricted to Host parameter for the group must be set to YES. Minimum length = 1
selectorvalue	<String>	Read-write	Value of the selector to be used for flushing objects from the content group. Requires that an invalidation selector be configured for the content group. Minimum length = 1
tosecondary	<String>	Read-write	content group whose objects are to be sent to secondary. Default value: NO

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = YES, NO
flags	<Integer>	Read-only	Flags.
prefetchcur	<Integer>	Read-only	Current outstanding prefetches.
memusage	<Integer>	Read-only	Current memory usage.
memdusage	<Integer>	Read-only	Current disk memory usage.
disklimit	<Integer>	Read-only	Maximum amount of disk that the cache can use. The effective limit is based on the available memory of the Citrix ADC. Default value: 0
cachenon304hits	<Integer>	Read-only	Cache non 304 hits.
cache304hits	<Integer>	Read-only	Cache 304 hits.
cachecells	<Integer>	Read-only	Number of cells.
cachegroupincarnation	<Integer>	Read-only	Cache group incarnation.
persist	<String>	Read-only	Setting persist to YES causes IC to save objects in contentgroup to disk. Default value: NO Possible values = YES, NO

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
policyname	<String[]>	Read-only	Active cache policies refering to this group.
cachenuminvalpolicy	<Integer>	Read-only	Number of active Invalidation policies refering to this group.
markercells	<Integer>	Read-only	Numbers of marker cells in this group.
builtin	<String[]>	Read-only	. Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL
feature	<String>	Read-only	The feature to be checked while applying this config.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT
- EXPIRE

- FLUSH
- SAVE

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/cachecontentgroup **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"cachecontentgroup":{

<b>"name":<String_value>,

</b>"weakposrelexpiry":<Integer_value>,

"heurexpiryparam":<Integer_value>,

"relexpiry":<Integer_value>,

"relexpirymillisec":<Integer_value>,

"absexpiry":<String[]_value>,

"absexpirygmt":<String[]_value>,

"weaknegrelexpiry":<Integer_value>,

"hitparams":<String[]_value>,

"invalparams":<String[]_value>,

"ignoreparamvaluecase":<String_value>,

"matchcookies":<String_value>,

"invalrestrictedtohost":<String_value>,

"polleverytime":<String_value>,

"ignorereloadreq":<String_value>,

"removecookies":<String_value>,

"prefetch":<String_value>,

"prefetchperiod":<Integer_value>,

"prefetchperiodmillisec":<Integer_value>,

"prefetchmaxpending":<Integer_value>,

"flashcache":<String_value>,
```

```
"expireatlastbyte":<String_value>,

"insertvia":<String_value>,

"insertage":<String_value>,

"insertetag":<String_value>,

"cachecontrol":<String_value>,

"quickabortsize":<Integer_value>,

"minressize":<Integer_value>,

"maxressize":<Integer_value>,

"memlimit":<Integer_value>,

"ignorereqcachinghdrs":<String_value>,

"minhits":<Integer_value>,

"alwaysevalpolicies":<String_value>,

"persistha":<String_value>,

"pinned":<String_value>,

"lazydnsresolve":<String_value>,

"hitselector":<String_value>,

"invalselector":<String_value>,

"type":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/cachecontentgroup/ name_value<String>
HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/cachecontentgroup **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"cachecontentgroup":{

<b>"name":<String_value>,

</b>"weakposrelexpiry":<Integer_value>,

"heurexpiryparam":<Integer_value>,

"relexpiry":<Integer_value>,

"relexpirymillisec":<Integer_value>,

"absexpiry":<String[]_value>,

"absexpirygmt":<String[]_value>,

"weaknegrelexpiry":<Integer_value>,
```

```
"hitparams":<String[]_value>,

"invalparams":<String[]_value>,

"ignoreparamvaluecase":<String_value>,

"matchcookies":<String_value>,

"invalrestrictedtohost":<String_value>,

"polleverytime":<String_value>,

"ignorereloadreq":<String_value>,

"removecookies":<String_value>,

"prefetch":<String_value>,

"prefetchperiod":<Integer_value>,

"prefetchperiodmillisec":<Integer_value>,

"prefetchmaxpending":<Integer_value>,

"flashcache":<String_value>,

"expireatlastbyte":<String_value>,

"insertvia":<String_value>,

"insertage":<String_value>,

"insertetag":<String_value>,

"cachecontrol":<String_value>,

"quickabortsize":<Integer_value>,

"minressize":<Integer_value>,

"maxressize":<Integer_value>,

"memlimit":<Integer_value>,
```

```
"ignorereqcachinghdrs":<String_value>,

"minhits":<Integer_value>,

"alwaysevalpolicies":<String_value>,

"persistha":<String_value>,

"pinned":<String_value>,

"lazydnsresolve":<String_value>,

"hitselector":<String_value>,

"invalselector":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/cachecontentgroup? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"cachecontentgroup":{

<b>"name":<String_value>,

</b>"weakposrelexpiry":true,
```

```
"heurexpiryparam":true,

"relexpiry":true,

"relexpirymillisec":true,

"absexpiry":true,

"absexpirygmt":true,

"weaknegrelexpiry":true,

"hitparams":true,

"invalparams":true,

"ignoreparamvaluecase":true,

"matchcookies":true,

"invalrestrictedtohost":true,

"polleverytime":true,

"ignorereloadreq":true,

"removecookies":true,

"prefetch":true,

"prefetchperiod":true,

"prefetchperiodmillisec":true,

"prefetchmaxpending":true,

"flashcache":true,

"expireatlastbyte":true,

"insertvia":true,

"insertage":true,
```

```
"insertetag":true,

"cachecontrol":true,

"quickabortsize":true,

"minressize":true,

"maxressize":true,

"memlimit":true,

"ignorereqcachinghdrs":true,

"minhits":true,

"alwaysevalpolicies":true,

"persistha":true,

"pinned":true,

"lazydnsresolve":true,

"hitselector":true,

"invalselector":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

EXPIRE

URL: http:// <netscaler-ip-address> /nitro/v1/config/cachecontentgroup? **action=expire HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"cachecontentgroup":{

<b>"name":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

FLUSH

URL: http:// <netscaler-ip-address> /nitro/v1/config/cachecontentgroup? **action=flush HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"cachecontentgroup":{

<b>"name":<String_value>,

</b>"query":<String_value>,

"host":<String_value>,

"selectorvalue":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

SAVE

URL: http:// <netscaler-ip-address> /nitro/v1/config/cachecontentgroup? **action=save HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"cachecontentgroup":{

<b>"name":<String_value>,

</b>"tosecondary":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/cachecontentgroup **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/cachecontentgroup? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/cachecontentgroup? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of cachecontentgroup resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/cachecontentgroup? **view=summary**

Use this query-parameter to get the summary output of cachecontentgroup resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/cachecontentgroup? **pagesize=#no;pageno=#no**

Use this query-parameter to get the cachecontentgroup resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "cachecontentgroup": [ {

"name":<String_value>,

"flags":<Integer_value>,

"type":<String_value>,

"relexpiry":<Integer_value>,

"relexpirymillisec":<Integer_value>,

"absexpiry":<String[]_value>,
```

```
"absexpirygmt":<String[]_value>,

"heurexpiryparam":<Integer_value>,

"weakposrelexpiry":<Integer_value>,

"weaknegrelexpiry":<Integer_value>,

"hitparams":<String[]_value>,

"invalparams":<String[]_value>,

"ignoreparamvaluecase":<String_value>,

"matchcookies":<String_value>,

"invalrestrictedtohost":<String_value>,

"polleverytime":<String_value>,

"ignorereloadreq":<String_value>,

"removecookies":<String_value>,

"prefetch":<String_value>,

"prefetchperiod":<Integer_value>,

"prefetchperiodmillisec":<Integer_value>,

"prefetchcur":<Integer_value>,

"prefetchmaxpending":<Integer_value>,

"flashcache":<String_value>,

"expireatlastbyte":<String_value>,

"insertvia":<String_value>,

"insertage":<String_value>,

"insertetag":<String_value>,
```

```
"cachecontrol":<String_value>,

"quickabortsize":<Integer_value>,

"minressize":<Integer_value>,

"maxressize":<Integer_value>,

"memusage":<Integer_value>,

"memdusage":<Integer_value>,

"disklimit":<Integer_value>,

"memlimit":<Integer_value>,

"ignorereqcachinghdrs":<String_value>,

"cachenon304hits":<Integer_value>,

"cache304hits":<Integer_value>,

"cachecells":<Integer_value>,

"cachegroupincarnation":<Integer_value>,

"minhits":<Integer_value>,

"alwaysevalpolicies":<String_value>,

"persist":<String_value>,

"persistha":<String_value>,

"pinned":<String_value>,

"lazydnsresolve":<String_value>,

"hitselector":<String_value>,

"invalselector":<String_value>,

"policyname":<String[]_value>,
```

```
"cachenuminvalpolicy":<Integer_value>,

"markercells":<Integer_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/cachecontentgroup/ name_value<String>
Query-parameters: attrs http:// <netscaler-ip-address> /nitro/v1/config/cachecontentgroup/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/cachecontentgroup/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of cachecontentgroup resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "cachecontentgroup": [ {

"name":<String_value>,

"flags":<Integer_value>,

"type":<String_value>,

"relexpiry":<Integer_value>,

"relexpirymillisec":<Integer_value>,

"absexpiry":<String[]_value>,

"absexpirygmt":<String[]_value>,

"heurexpiryparam":<Integer_value>,

"weakposrelexpiry":<Integer_value>,

"weaknegrelexpiry":<Integer_value>,

"hitparams":<String[]_value>,

"invalparams":<String[]_value>,

"ignoreparamvaluecase":<String_value>,

"matchcookies":<String_value>,

"invalrestrictedtohost":<String_value>,

"polleverytime":<String_value>,

"ignorereloadreq":<String_value>,

"removecookies":<String_value>,

"prefetch":<String_value>,
```

```
"prefetchperiod":<Integer_value>,

"prefetchperiodmillisec":<Integer_value>,

"prefetchcur":<Integer_value>,

"prefetchmaxpending":<Integer_value>,

"flashcache":<String_value>,

"expireatlastbyte":<String_value>,

"insertvia":<String_value>,

"insertage":<String_value>,

"insertetag":<String_value>,

"cachecontrol":<String_value>,

"quickabortsize":<Integer_value>,

"minressize":<Integer_value>,

"maxressize":<Integer_value>,

"memusage":<Integer_value>,

"memdusage":<Integer_value>,

"disklimit":<Integer_value>,

"memlimit":<Integer_value>,

"ignorereqcachinghdrs":<String_value>,

"cachenon304hits":<Integer_value>,

"cache304hits":<Integer_value>,

"cachecells":<Integer_value>,

"cachegroupincarnation":<Integer_value>,
```

```
"minhits":<Integer_value>,

"alwaysevalpolicies":<String_value>,

"persist":<String_value>,

"persistha":<String_value>,

"pinned":<String_value>,

"lazydnsresolve":<String_value>,

"hitselector":<String_value>,

"invalselector":<String_value>,

"policyname":<String[]_value>,

"cachenuminvalpolicy":<Integer_value>,

"markercells":<Integer_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/cachecontentgroup? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "cachecontentgroup": [ { "__count": "#no"} ] }
```

cacheforwardproxy

Configuration for forward proxy resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ipaddress	<String>	Read-write	IP address of the Citrix ADC or a cache server for which the cache acts as a proxy. Requests coming to the Citrix ADC with the configured IP address are forwarded to the particular address, without involving the Integrated Cache in any way. Minimum length = 1
port	<Integer>	Read-write	Port on the Citrix ADC or a server for which the cache acts as a proxy.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum value = 1 Range 1 - 65535 * in CLI is represented as 65535 in NITRO API
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/cacheforwardproxy **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"cacheforwardproxy":{

<b>"ipaddress":<String_value>,

</b><b>"port":<Integer_value>

</b>}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/cacheforwardproxy/ ipaddress_value<String>
Query-parameters: args= port:<Integer_value>

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/cacheforwardproxy **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/cacheforwardproxy? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/cacheforwardproxy? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of cacheforwardproxy resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/cacheforwardproxy? **view=summary**

Use this query-parameter to get the summary output of cacheforwardproxy resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/cacheforwardproxy? **pagesize=#no;pageno=#no**

Use this query-parameter to get the cacheforwardproxy resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "cacheforwardproxy": [ {

"ipaddress":<String_value>,

"port":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/cacheforwardproxy? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "cacheforwardproxy": [ { "__count": "#no"} ] }
```

cacheglobal_binding

Binding object which returns the resources bound to cacheglobal.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
cacheglobal_cachepolicy_binding	<cacheglobal_cachepolicy_binding[]>	Read-write	cachepolicy that can be bound to cacheglobal.

Operations

(click to see Properties)

- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/cacheglobal_binding

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "cacheglobal_binding": [ {

"cacheglobal_cachepolicy_binding":<cacheglobal_cachepolicy_binding[]_value
>

}]}
```

cacheglobal_cachepolicy_binding

Binding object showing the cachepolicy that can be bound to cacheglobal.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
priority	<Integer>	Read-write	Specifies the priority of the policy.
labeltype	<String>	Read-write	Type of policy label to invoke. Possible values = reqvserver, resvserver, policylabel
labelname	<String>	Read-write	Name of the label to invoke if the current policy rule evaluates to TRUE. (To invoke a label associated with a virtual server, specify the name of the virtual server.).
precededefrules	<String>	Read-write	Specify whether this policy should be evaluated. Default value: NO Possible values = YES, NO
type	<String>	Read-write	The bind point to which policy is bound. When you specify the type, detailed information about that bind point appears. Possible values = REQ_OVERRIDE, REQ_DEFAULT, RES_OVERRIDE, RES_DEFAULT,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			HTTPQUIC_REQ_OVERRIDE, HTTPQUIC_REQ_DEFAULT, HTTPQUIC_RES_OVERRIDE, HTTPQUIC_RES_DEFAULT
invoke	<Boolean>	Read-write	Invoke policies bound to a virtual server or a user-defined policy label. After the invoked policies are evaluated, the flow returns to the policy with the next priority. Applicable only to default-syntax policies.
gotopriorityexpression	<String>	Read-write	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
policy	<String>	Read-write	Name of the cache policy.
globalbindtype	<String>	Read-write	. Default value: SYSTEM_GLOBAL Possible values = SYSTEM_GLOBAL, VPN_GLOBAL,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			RNAT_GLOBAL, APPFW_GLOBAL, TM_GLOBAL
numpol	<Integer>	Read-only	The number of policies bound to the bindpoint.
flowtype	<Integer>	Read-only	flowtype of the bound cache policy.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/cacheglobal_cachepolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"cacheglobal_cachepolicy_binding":{

<b>"policy":<String_value>,

</b><b>"priority":<Integer_value>,

</b>"precededefrules":<String_value>,

"gotopriorityexpression":<String_value>,

"type":<String_value>,

"invoke":<Boolean_value>,

"labeltype":<String_value>,

"labelname":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/cacheglobal_cachepolicy_binding **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/cacheglobal_cachepolicy_binding? **args= policy:<String_value>, type: <String_value> ,priority: <Integer_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/cacheglobal_cachepolicy_binding **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/cacheglobal_cachepolicy_binding? **args=type: <String_value>**

Use this query-parameter to get cacheglobal_cachepolicy_binding resources based on additional properties.

filter http:// <netscaler-ip-address> /nitro/v1/config/cacheglobal_cachepolicy_binding? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of cacheglobal_cachepolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/cacheglobal_cachepolicy_binding? **pagesize=#no;pageno=#no**

Use this query-parameter to get the cacheglobal_cachepolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "cacheglobal_cachepolicy_binding": [ {

"priority":<Integer_value>,

"labeltype":<String_value>,

"labelname":<String_value>,

"precededefrules":<String_value>,

"type":<String_value>,

"invoke":<Boolean_value>,

"gotopriorityexpression":<String_value>,

"policy":<String_value>,

"globalbindtype":<String_value>,

"numpol":<Integer_value>,

"flowtype":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/cacheglobal_cachepolicy_binding? **count=yes**
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "cacheglobal_cachepolicy_binding": [ { "__count": "#no"} ] }
```

cacheobject

Configuration for cache object resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
url	<String>	Read-write	URL of the particular object whose details is required. Parameter "host" must be specified along with the URL. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
locator	<Integer>	Read-write	ID of the cached object.
httpstatus	<Integer>	Read-write	HTTP status of the object.
host	<String>	Read-write	Host name of the object. Parameter "url" must be specified. Minimum length = 1
port	<Integer>	Read-write	Host port of the object. You must also set the Host parameter. Default value: 80 Minimum value = 1
groupname	<String>	Read-write	Name of the content group to which the object belongs. It will display only the objects belonging to the specified content group. You must also set the Host parameter.
httpmethod	<String>	Read-write	HTTP request method that caused the object to be stored. Default value: GET Possible values = GET, POST

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
group	<String>	Read-write	Name of the content group whose objects should be listed.
ignoremarkerobjects	<String>	Read-write	Ignore marker objects. Marker objects are created when a response exceeds the maximum or minimum response size for the content group or has not yet received the minimum number of hits for the content group. Possible values = ON, OFF
includenotreadyobjects	<String>	Read-write	Include responses that have not yet reached a minimum number of hits before being cached. Possible values = ON, OFF
nodeid	<Integer>	Read-write	Unique number that identifies the cluster node. Minimum value = 0 Maximum value = 31
tosecondary	<String>	Read-write	Object will be saved onto Secondary. Default value: NO

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = YES, NO
cacheressize	<Integer>	Read-only	Cache response size of the object.
cachereshdrsize	<Integer>	Read-only	Cache response header size of the object.
cacheetag	<String>	Read-only	Cache ETag of the object.
httpstatusoutput	<Integer>	Read-only	HTTP status of the object.
cachereslastmod	<String>	Read-only	Value of "Last-modified" header.
cachecontrol	<String>	Read-only	Cache-Control header of the object.
cacheresdate	<String>	Read-only	Value of "Date" header.
contentgroup	<String>	Read-only	Name of the contentgroup in which it is stored.
destipv46	<String>	Read-only	Destination IP.
destport	<Integer>	Read-only	Destination Port. Range 1 - 65535 * in CLI is represented as 65535 in NITRO API

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
cachecellcomplex	<String>	Read-only	The state of the parameterized caching on this cell. Possible values = YES, NO
hitparams	<String[]>	Read-only	Parameterized hit evaluation of an object.
hitvalues	<String[]>	Read-only	Values of hitparams for this object.
cachecellreqtime	<Integer>	Read-only	Required time of the cache cell object.
cachecellrestime	<Integer>	Read-only	Response time to the cache cell object.
cachecurage	<Integer>	Read-only	Current age of the cache object.
cachecellexpires	<Integer>	Read-only	Expiry time of the cache cell object in seconds.
cachecellexpiresmillisec	<Integer>	Read-only	Expiry time of the cache cell object in milliseconds.
flushed	<String>	Read-only	Specifies whether the object is flushed. Possible values = YES, NO
prefetch	<String>	Read-only	Specifies whether Integrated Cache should attempt to refresh an object immediately before it goes stale.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = YES, NO
prefetchperiod	<Integer>	Read-only	The duration in seconds of the period during which prefetch should be attempted, immediately before the object's calculated expiry time.
prefetchperiodmillisec	<Integer>	Read-only	The duration in milliseconds of the period during which prefetch should be attempted, immediately before the object's calculated expiry time.
cachecellcurreaders	<Integer>	Read-only	Current readers of the cache cell object.
cachecellcurmisses	<Integer>	Read-only	Current misses of the cache cell object.
cachecellhits	<Integer>	Read-only	Cache cell hits.
cachecellmisses	<Integer>	Read-only	Cache cell misses.
cachecelldhits	<Integer>	Read-only	Cache cell disk hits.
cachecellcompressionformat	<String>	Read-only	Compression format of this object. Identity means not compressed.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
cachecellappfwmetadataexists	<String>	Read-only	AppFirewall cache object. Possible values = YES, NO
cachecellhttp11	<String>	Read-only	The state of the response to be HTTP/1.1. Possible values = YES, NO
cachecellweaketag	<String>	Read-only	The state of the weak HTTP Entity Tag in the cell. Possible values = YES, NO
cachecellresbadsize	<String>	Read-only	The marked state of the cell. Possible values = YES, NO
markerreason	<String>	Read-only	Reason for marking the cell. Possible values = Waiting for min hit, Response header is too big, Content-length header said response size is not in group size limit, Content-length response received more data, Content-length response received less data, Content-length response data is not

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			in group size limit, Chunk response received more data, Chunk response data is not in group size limit, Bad chunk format, Fin terminated response data is not in group size limit
cachecellpolleverytime	<String>	Read-only	The state to poll every time on object. Possible values = YES, NO
cachecelletaginserted	<String>	Read-only	The state of the ETag to be inserted by IC for this object. Possible values = YES, NO
cachecellreadywithlastbyte	<String>	Read-only	The state of the complete arrived response. Possible values = YES, NO
cacheinmemory	<String>	Read-only	The cache data is available in memory. Possible values = YES, NO
cacheindisk	<String>	Read-only	The cache data is available in disk. Possible values = YES, NO

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
cacheinsecondary	<String>	Read-only	The cache data is available in secondary in HA deployment. Possible values = YES, NO
cachedirname	<String>	Read-only	The directory name used if saved.
cachefilename	<String>	Read-only	The filename used if saved.
cachecelldestipverified	<String>	Read-only	The state of DNS verification. Possible values = YES, NO
cachecellfwpxyobj	<String>	Read-only	The state of the object to be stored on a request to a forward proxy. Possible values = YES, NO
cachecellbasefile	<String>	Read-only	The state of delta being used as a basefile. Possible values = YES, NO
cachecellminhitflag	<String>	Read-only	The state of the minhit feature on this cell. Possible values = YES, NO
cachecellminhit	<Integer>	Read-only	Min hit value for the object.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
policy	<Integer>	Read-only	Policy info for the object.
policyname	<String>	Read-only	Policy which created the object.
selectorname	<String[]>	Read-only	The hit selector for the object.
rule	<String[]>	Read-only	Selectors for this object.
selectorvalue	<String[]>	Read-only	The HTTP request method that caused the object to be stored.
cacheurls	<String>	Read-only	List of cache object URLs.
warnbucketskip	<Integer>	Read-only	Bucket skipped warning.
totalobjs	<Integer>	Read-only	Total objects.
httpcalloutcell	<String>	Read-only	Is it a http callout cell ?. Possible values = YES, NO
httpcalloutname	<String>	Read-only	Name of the http callout.
returntype	<String>	Read-only	Return type of the http callout. Possible values = BOOL, NUM, TEXT
httpcalloutresult	<String>	Read-only	First few bytes of http callout response.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
locatorshow	<Integer>	Read-only	ID of the cached object.
ceflags	<Integer>	Read-only	Indicates state and type of cached cell.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET (ALL)
- COUNT
- EXPIRE
- FLUSH
- SAVE

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

EXPIRE

URL: http:// <netscaler-ip-address> /nitro/v1/config/cacheobject? **action=expire HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"cacheobject":{

"locator":<Integer_value>,

"url":<String_value>,

"host":<String_value>,

"port":<Integer_value>,

"groupname":<String_value>,

"httpmethod":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

FLUSH

URL: http:// <netscaler-ip-address> /nitro/v1/config/cacheobject? **action=flush HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"cacheobject":{

"locator":<Integer_value>,

"url":<String_value>,

"host":<String_value>,

"port":<Integer_value>,

"groupname":<String_value>,

"httpmethod":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

SAVE

URL: http:// <netscaler-ip-address> /nitro/v1/config/cacheobject? **action=save HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"cacheobject":{

"locator":<Integer_value>,

"tosecondary":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/cacheobject **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/cacheobject? **args=url: <String_value> ,locator: <Integer_value> ,httpstatus: <Integer_value> ,host: <String_value> ,port: <Integer_value> ,groupname: <String_value> ,httpmethod: <String_value> ,group: <String_value> ,ignoremarkerobjects: <String_value> ,includenotreadyobjects: <String_value> ,nodeid: <Integer_value>**

Use this query-parameter to get cacheobject resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/config/cacheobject? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/cacheobject? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of cacheobject resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/cacheobject? **view=summary**

Use this query-parameter to get the summary output of cacheobject resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/cacheobject?
pagesize=#no;pageno=#no

Use this query-parameter to get the cacheobject resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "cacheobject": [ {

url:<String_value>,locator:<Integer_value>,httpstatus:<Integer_value>,host
:<String_value>,port:<Integer_value>,groupname:<String_value>,httpmethod:<
String_value>,group:<String_value>,ignoremarkerobjects:<String_value>,incl
udenotreadyobjects:<String_value>,nodeid:<Integer_value>"cacheressize":<In
teger_value>,

"cachereshdrsize":<Integer_value>,

"cacheetag":<String_value>,

"httpstatusoutput":<Integer_value>,

"cachereslastmod":<String_value>,

"cachecontrol":<String_value>,

"cacheresdate":<String_value>,
```

```
"contentgroup":<String_value>,

"destip":<Integer_value>,

"destipv46":<String_value>,

"destport":<Integer_value>,

"cachecellcomplex":<String_value>,

"hitparams":<String[]_value>,

"hitvalues":<String[]_value>,

"cachecellreqtime":<Integer_value>,

"cachecellrestime":<Integer_value>,

"cachecurage":<Integer_value>,

"cachecellexpires":<Integer_value>,

"cachecellexpiresmillisec":<Integer_value>,

"flushed":<String_value>,

"prefetch":<String_value>,

"prefetchperiod":<Integer_value>,

"prefetchperiodmillisec":<Integer_value>,

"cachecellcurreaders":<Integer_value>,

"cachecellcurmisses":<Integer_value>,

"cachecellhits":<Integer_value>,

"cachecellmisses":<Integer_value>,

"cachecelldhits":<Integer_value>,

"cachecellgzipcompressed":<String_value>,
```

```
"cachecelldeflatecompressed":<String_value>,

"cachecellcompressionformat":<String_value>,

"cachecellappfwmetadataexists":<String_value>,

"cachecellhttp11":<String_value>,

"cachecellweaketag":<String_value>,

"cachecellresbadsize":<String_value>,

"markerreason":<String_value>,

"cachecellpolleverytime":<String_value>,

"cachecelletaginserted":<String_value>,

"cachecellreadywithlastbyte":<String_value>,

"cacheinmemory":<String_value>,

"cacheindisk":<String_value>,

"cacheinsecondary":<String_value>,

"cachedirname":<String_value>,

"cachefilename":<String_value>,

"cachecelldestipverified":<String_value>,

"cachecellfwpxyobj":<String_value>,

"cachecellbasefile":<String_value>,

"cachecellminhitflag":<String_value>,

"cachecellminhit":<Integer_value>,

"policy":<Integer_value>,

"policyname":<String_value>,
```

```
"selectorname":<String[]_value>,

"rule":<String[]_value>,

"selectorvalue":<String[]_value>,

"cacheurls":<String_value>,

"warnbucketskip":<Integer_value>,

"totalobjs":<Integer_value>,

"httpcalloutcell":<String_value>,

"httpcalloutname":<String_value>,

"returntype":<String_value>,

"httpcalloutresult":<String_value>,

"locatorshow":<Integer_value>,

"ceflags":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/cacheobject? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "cacheobject": [ { "__count": "#no"} ] }
```

cacheparameter

Configuration for cache parameter resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
memlimit	<Integer>	Read-write	Amount of memory available for storing the cache objects. In practice, the amount of memory available for caching can be less than half the total memory of the Citrix ADC.
via	<String>	Read-write	String to include in the Via header. A Via header is inserted into all responses served from a content group if its Insert Via flag is set. Minimum length = 1
verifyusing	<String>	Read-write	Criteria for deciding whether a cached object can be served for an incoming HTTP request.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Available settings function as follows: HOSTNAME - The URL, host name, and host port values in the incoming HTTP request header must match the cache policy. The IP address and the TCP port of the destination host are not evaluated. Do not use the HOSTNAME setting unless you are certain that no rogue client can access a rogue server through the cache. HOSTNAME_AND_IP - The URL, host name, host port in the incoming HTTP request header, and the IP address and TCP port of the destination server, must match the cache policy. DNS - The URL, host name and host port in the incoming

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			HTTP request, and the TCP port must match the cache policy. The host name is used for DNS lookup of the destination server's IP address, and is compared with the set of addresses returned by the DNS lookup. Possible values = HOSTNAME, HOSTNAME_AND_IP, DNS
maxpostlen	<Integer>	Read-write	Maximum number of POST body bytes to consider when evaluating parameters for a content group for which you have configured hit parameters and invalidation parameters. Default value: 4096 Minimum value = 0 Maximum value = 131072
prefetchmaxpending	<Integer>	Read-write	Maximum number of outstanding

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			prefetches in the Integrated Cache.
enablebypass	<String>	Read-write	Evaluate the request-time policies before attempting hit selection. If set to NO, an incoming request for which a matching object is found in cache storage results in a response regardless of the policy configuration. If the request matches a policy with a NOCACHE action, the request bypasses all cache processing. This parameter does not affect processing of requests that match any invalidation policy. Possible values = YES, NO
undefaction	<String>	Read-write	Action to take when a policy cannot be evaluated. Possible values = NOCACHE, RESET

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
enablehaobjpersist	<String>	Read-write	The HA object persisting parameter. When this value is set to YES, cache objects can be synced to Secondary in a HA deployment. If set to NO, objects will never be synced to Secondary node. Default value: NO Possible values = YES, NO
cacheevictionpolicy	<String>	Read-write	The cacheEvictionPolicy determines the threshold for preemptive eviction of cache objects using the LRU (Least Recently Used) algorithm. If set to AGGRESSIVE, eviction is triggered when free cache memory drops to 40%. MODERATE triggers eviction at 25%, and RELAXED triggers eviction at 10%. Default value: RELAXED Possible values = RELAXED, MODERATE, AGGRESSIVE

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
disklimit	<Integer>	Read-only	The disk limit for the Integrated Cache.
maxdisklimit	<Integer>	Read-only	The maximum value of the memory limit for the Integrated Cache.
memlimitactive	<Integer>	Read-only	Active value of the memory limit for the Integrated Cache.
maxmemlimit	<Integer>	Read-only	The maximum value of the memory limit for the Integrated Cache.
prefetchcur	<Integer>	Read-only	Number of current outstanding prefetches in the IC.
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- UPDATE
- UNSET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/cacheparameter **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"cacheparameter":{

"memlimit":<Integer_value>,

"via":<String_value>,

"verifyusing":<String_value>,

"maxpostlen":<Integer_value>,

"prefetchmaxpending":<Integer_value>,

"enablebypass":<String_value>,

"undefaction":<String_value>,
```

```
"enablehaobjpersist":<String_value>,

"cacheevictionpolicy":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/cacheparameter? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"cacheparameter":{

"memlimit":true,

"via":true,

"verifyusing":true,

"maxpostlen":true,

"prefetchmaxpending":true,

"enablebypass":true,

"undefaction":true,

"enablehaobjpersist":true,
```

```
"cacheevictionpolicy":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/cacheparameter **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "cacheparameter": [ {

"disklimit":<Integer_value>,

"maxdisklimit":<Integer_value>,

"memlimit":<Integer_value>,

"memlimitactive":<Integer_value>,

"maxmemlimit":<Integer_value>,

"via":<String_value>,
```

```
"verifyusing":<String_value>,

"maxpostlen":<Integer_value>,

"prefetchcur":<Integer_value>,

"prefetchmaxpending":<Integer_value>,

"enablebypass":<String_value>,

"undefaction":<String_value>,

"enablehaobjpersist":<String_value>,

"cacheevictionpolicy":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

cachepolicy

Configuration for Integrated Cache policy resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
policyname	<String>	Read-write	Name for the policy. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			characters. Can be changed after the policy is created. Minimum length = 1
rule	<String>	Read-write	Expression against which the traffic is evaluated. The following requirements apply only to the Citrix ADC CLI: * If the expression includes one or more spaces, enclose the entire expression in double quotation marks. * If the expression itself includes double quotation marks, escape the quotations by using the \ character. * Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
action	<String>	Read-write	Action to apply to content that matches the policy. * CACHE or MAY_CACHE action - positive cachability policy * NOCACHE or MAY_NOCACHE action - negative cachability policy * INVAL action - Dynamic Invalidation Policy. Possible values = CACHE, NOCACHE, MAY_CACHE, MAY_NOCACHE, INVAL
storeingroup	<String>	Read-write	Name of the content group in which to store the object when the final result of policy evaluation is CACHE. The content group must exist before being mentioned here. Use the "show cache contentgroup" command to view the list of existing content groups. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
invalgroups	<String[]>	Read-write	Content group(s) to be invalidated when the INVAL action is applied. Maximum number of content groups that can be specified is 16. Minimum length = 1
invalobjects	<String[]>	Read-write	Content groups(s) in which the objects will be invalidated if the action is INVAL. Minimum length = 1
undefaction	<String>	Read-write	Action to be performed when the result of rule evaluation is undefined. Possible values = NOCACHE, RESET
newname	<String>	Read-write	New name for the cache policy. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Minimum length = 1
hits	<Integer>	Read-only	Hits.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
undefhits	<Integer>	Read-only	Number of Undef hits.
flags	<Integer>	Read-only	Flag.
builtin	<String[]>	Read-only	. Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL
feature	<String>	Read-only	The feature to be checked while applying this config.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT
- RENAME

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/cachepolicy **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"cachepolicy":{

<b>"policyname":<String_value>,

</b><b>"rule":<String_value>,

</b><b>"action":<String_value>,

</b>"storeingroup":<String_value>,

"invalgroups":<String[]_value>,
```

```
"invalobjects":<String[]_value>,

"undefaction":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/cachepolicy/ policyname_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/cachepolicy **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"cachepolicy":{

<b>"policyname":<String_value>,

</b>"rule":<String_value>,

"action":<String_value>,
```

```
"storeingroup":<String_value>,

"invalgroups":<String[]_value>,

"invalobjects":<String[]_value>,

"undefaction":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/cachepolicy? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"cachepolicy":{

<b>"policyname":<String_value>,

</b>"storeingroup":true,

"invalgroups":true,

"invalobjects":true,

"undefaction":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

RENAME

URL: http:// <netscaler-ip-address> /nitro/v1/config/cachepolicy? **action=rename HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"cachepolicy":{

<b>"policyname":<String_value>,

</b><b>"newname":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/cachepolicy **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/cachepolicy? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/cachepolicy? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of cachepolicy resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/cachepolicy? **view=summary**

Use this query-parameter to get the summary output of cachepolicy resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/cachepolicy? **pagesize=#no;pageno=#no**

Use this query-parameter to get the cachepolicy resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "cachepolicy": [ {

"policyname":<String_value>,

"rule":<String_value>,

"action":<String_value>,

"storeingroup":<String_value>,

"invalgroups":<String[]_value>,
```

```
"invalobjects":<String[]_value>,

"hits":<Integer_value>,

"undefaction":<String_value>,

"undefhits":<Integer_value>,

"flags":<Integer_value>,

"precededefrules":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/cachepolicy/ policyname_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/cachepolicy/ policyname_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/cachepolicy/ policyname_value<String> ? **view=summary**

Use this query-parameter to get the summary output of cachepolicy resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "cachepolicy": [ {

"policyname":<String_value>,

"rule":<String_value>,

"action":<String_value>,

"storeingroup":<String_value>,

"invalgroups":<String[]_value>,

"invalobjects":<String[]_value>,

"hits":<Integer_value>,

"undefaction":<String_value>,

"undefhits":<Integer_value>,

"flags":<Integer_value>,

"precededefrules":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

```
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/cachepolicy? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "cachepolicy": [ { "__count": "#no"} ] }
```

cachepolicy_binding

Binding object which returns the resources bound to cachepolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
policyname	<String>	Read-write	Name of the cache policy about which to display details. Minimum length = 1
cachepolicy_lbvserver_binding	<cachepolicy_lbvserver_binding[]>	Read-only	lbvserver that can be bound to cachepolicy.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
cachepolicy_cachegl obal_binding	<cachepolicy_cache global_binding[]>	Read-only	cacheglobal that can be bound to cachepolicy.
cachepolicy_cachep olicylabel_binding	<cachepolicy_cache policylabel_binding[] >	Read-only	cachepolicylabel that can be bound to cachepolicy.
cachepolicy_csvserv er_binding	<cachepolicy_csvser ver_binding[]>	Read-only	csvserver that can be bound to cachepolicy.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/cachepolicy_binding/ policyname_value<String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "cachepolicy_binding": [ {

"policyname":<String_value>,

"cachepolicy_csvserver_binding":<cachepolicy_csvserver_binding[]_value>,

"cachepolicy_lbvserver_binding":<cachepolicy_lbvserver_binding[]_value>,

"cachepolicy_cacheglobal_binding":<cachepolicy_cacheglobal_binding[]_value
>,

"cachepolicy_cachepolicylabel_binding":<cachepolicy_cachepolicylabel_bindi
ng[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/cachepolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/cachepolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "cachepolicy_binding": [ {

"policyname":<String_value>,

"cachepolicy_csvserver_binding":<cachepolicy_csvserver_binding[]_value>,

"cachepolicy_lbvserver_binding":<cachepolicy_lbvserver_binding[]_value>,

"cachepolicy_cacheglobal_binding":<cachepolicy_cacheglobal_binding[]_value
>,

"cachepolicy_cachepolicylabel_binding":<cachepolicy_cachepolicylabel_bindi
ng[]_value>

}]}
```

cachepolicy_cacheglobal_binding

Binding object showing the cacheglobal that can be bound to cachepolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
policyname	<String>	Read-write	Name of the cache policy about which to display details. Minimum length = 1
boundto	<String>	Read-write	Location where policy is bound.
priority	<Integer>	Read-only	Priority.
labeltype	<String>	Read-only	Type of policy label invocation. Possible values = reqvserver, resvserver, policylabel
activepolicy	<Integer>	Read-only	Indicates whether policy is bound or not.
gotopriorityexpression	<String>	Read-only	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
labelname	<String>	Read-only	Name of the label to invoke if the current policy rule evaluates to TRUE.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/cachepolicy_cacheglobal_binding/ policyname_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ cachepolicy_cacheglobal_binding/ policyname_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of cachepolicy_cacheglobal_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/cachepolicy_cacheglobal_binding/ policyname_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the cachepolicy_cacheglobal_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "cachepolicy_cacheglobal_binding": [ {

"policyname":<String_value>,

"boundto":<String_value>,

"priority":<Integer_value>,

"labeltype":<String_value>,

"activepolicy":<Integer_value>,
```

```
"gotopriorityexpression":<String_value>,

"labelname":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/cachepolicy_cacheglobal_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/cachepolicy_cacheglobal_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "cachepolicy_cacheglobal_binding": [ {

"policyname":<String_value>,

"boundto":<String_value>,

"priority":<Integer_value>,
```

```
"labeltype":<String_value>,

"activepolicy":<Integer_value>,

"gotopriorityexpression":<String_value>,

"labelname":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/cachepolicy_cacheglobal_binding/ policyname_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"cachepolicy_cacheglobal_binding": [ { "__count": "#no"} ] }
```

cachepolicy_cachepolicylabel_binding

Binding object showing the cachepolicylabel that can be bound to cachepolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
policyname	<String>	Read-write	Name of the cache policy about which to display details. Minimum length = 1
boundto	<String>	Read-write	Location where policy is bound.
priority	<Integer>	Read-only	Priority.
labeltype	<String>	Read-only	Type of policy label invocation. Possible values = reqvserver, resvserver, policylabel
activepolicy	<Integer>	Read-only	Indicates whether policy is bound or not.
gotopriorityexpression	<String>	Read-only	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
labelname	<String>	Read-only	Name of the label to invoke if the current policy rule evaluates to TRUE.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET

- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/cachepolicy_cachepolicylabel_binding/ policyname_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ cachepolicy_cachepolicylabel_binding/ policyname_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of cachepolicy_cachepolicylabel_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/cachepolicy_cachepolicylabel_binding/ policyname_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the cachepolicy_cachepolicylabel_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "cachepolicy_cachepolicylabel_binding": [ {

"policyname":<String_value>,

"boundto":<String_value>,

"priority":<Integer_value>,

"labeltype":<String_value>,

"activepolicy":<Integer_value>,

"gotopriorityexpression":<String_value>,

"labelname":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/cachepolicy_cachepolicylabel_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/cachepolicy_cachepolicylabel_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "cachepolicy_cachepolicylabel_binding": [ {

"policyname":<String_value>,

"boundto":<String_value>,

"priority":<Integer_value>,

"labeltype":<String_value>,

"activepolicy":<Integer_value>,

"gotopriorityexpression":<String_value>,

"labelname":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/cachepolicy_cachepolicylabel_binding/policyname_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"cachepolicy_cachepolicylabel_binding": [ { "__count": "#no"} ] }
```

cachepolicy_csvserver_binding

Binding object showing the csvserver that can be bound to cachepolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
boundto	<String>	Read-write	Location where policy is bound.
policyname	<String>	Read-write	Name of the cache policy about which to display details. Minimum length = 1
labeltype	<String>	Read-only	Type of policy label invocation.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = reqvserver, resvserver, policylabel
priority	<Integer>	Read-only	Priority.
labelname	<String>	Read-only	Name of the label to invoke if the current policy rule evaluates to TRUE.
gotopriorityexpression	<String>	Read-only	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
activepolicy	<Integer>	Read-only	Indicates whether policy is bound or not.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/cachepolicy_csvserver_binding/ policyname_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ cachepolicy_csvserver_binding/ policyname_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of cachepolicy_csvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/cachepolicy_csvserver_binding/ policyname_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the cachepolicy_csvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "cachepolicy_csvserver_binding": [ {

"boundto":<String_value>,

"policyname":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"labelname":<String_value>,

"gotopriorityexpression":<String_value>,

"activepolicy":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/cachepolicy_csvserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/cachepolicy_csvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "cachepolicy_csvserver_binding": [ {

"boundto":<String_value>,

"policyname":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"labelname":<String_value>,

"gotopriorityexpression":<String_value>,

"activepolicy":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/cachepolicy_csvserver_binding/ policyname_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"cachepolicy_csvserver_binding": [ { "__count": "#no"} ] }
```

cachepolicy_lbvserver_binding

Binding object showing the lbvserver that can be bound to cachepolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
policyname	<String>	Read-write	Name of the cache policy about which to display details. Minimum length = 1
boundto	<String>	Read-write	Location where policy is bound.
labeltype	<String>	Read-only	Type of policy label invocation. Possible values = reqvserver, resvserver, policylabel
priority	<Integer>	Read-only	Priority.
labelname	<String>	Read-only	Name of the label to invoke if the current policy rule evaluates to TRUE.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
gotopriorityexpression	<String>	Read-only	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
activepolicy	<Integer>	Read-only	Indicates whether policy is bound or not.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/cachepolicy_lbvserver_binding/ policyname_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ cachepolicy_lbvserver_binding/ policyname_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of cachepolicy_lbvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/cachepolicy_lbvserver_binding/ policyname_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the cachepolicy_lbvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "cachepolicy_lbvserver_binding": [ {

"policyname":<String_value>,

"boundto":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"labelname":<String_value>,

"gotopriorityexpression":<String_value>,

"activepolicy":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/cachepolicy_lbvserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/cachepolicy_lbvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "cachepolicy_lbvserver_binding": [ {

"policyname":<String_value>,

"boundto":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"labelname":<String_value>,

"gotopriorityexpression":<String_value>,

"activepolicy":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/cachepolicy_lbvserver_binding/ policyname_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"cachepolicy_lbvserver_binding": [ { "__count": "#no"} ] }
```

cachepolicylabel

Configuration for cache policy label resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
labelname	<String>	Read-write	Name for the label. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Can be changed after the label is created.
evaluates	<String>	Read-write	When to evaluate policies bound to this label: request-time or response-time. Possible values = REQ, RES, MSSQL_REQ, MSSQL_RES, MYSQL_REQ, MYSQL_RES, HTTPQUIC_REQ, HTTPQUIC_RES

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
newname	<String>	Read-write	New name for the cache-policy label. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Minimum length = 1
numpol	<Integer>	Read-only	Number of polices bound to label.
hits	<Integer>	Read-only	Number of times policy label was invoked.
priority	<Integer>	Read-only	Specifies the priority of the policy.
gotopriorityexpression	<String>	Read-only	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
labeltype	<String>	Read-only	Type of policy label to invoke: an unnamed label associated with a virtual server, or user-defined policy label.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = reqvserver, resvserver, policylabel
invoke_labelname	<String>	Read-only	Name of the policy label to invoke if the current policy rule evaluates to TRUE.
flowtype	<Integer>	Read-only	Flowtype of the bound cache policy.
builtin	<String[]>	Read-only	. Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL
feature	<String>	Read-only	The feature to be checked while applying this config.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET (ALL)
- GET
- COUNT
- RENAME

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/cachepolicylabel **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"cachepolicylabel":{

<b>"labelname":<String_value>,

</b><b>"evaluates":<String_value>
```

```
</b>}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/cachepolicylabel/ labelname_value<String>
HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

RENAME

URL: http:// <netscaler-ip-address> /nitro/v1/config/cachepolicylabel? **action=rename HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"cachepolicylabel":{

<b>"labelname":<String_value>,

</b><b>"newname":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/cachepolicylabel **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/cachepolicylabel? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/cachepolicylabel? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of cachepolicylabel resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/cachepolicylabel? **view=summary**

Use this query-parameter to get the summary output of cachepolicylabel resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/cachepolicylabel? **pagesize=#no;pageno=#no**

Use this query-parameter to get the cachepolicylabel resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "cachepolicylabel": [ {

"labelname":<String_value>,

"evaluates":<String_value>,

"numpol":<Integer_value>,

"hits":<Integer_value>,

"priority":<Integer_value>,

"gotopriorityexpression":<String_value>,

"labeltype":<String_value>,

"invoke_labelname":<String_value>,

"flowtype":<Integer_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/cachepolicylabel/ labelname_value<String>
Query-parameters: attrs http:// <netscaler-ip-address> /nitro/v1/config/cachepolicylabel/ labelname_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/cachepolicylabel/ labelname_value<String> ? **view=summary**

Use this query-parameter to get the summary output of cachepolicylabel resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "cachepolicylabel": [ {

"labelname":<String_value>,

"evaluates":<String_value>,

"numpol":<Integer_value>,

"hits":<Integer_value>,

"priority":<Integer_value>,

"gotopriorityexpression":<String_value>,

"labeltype":<String_value>,

"invoke_labelname":<String_value>,

"flowtype":<Integer_value>,
```

```
"builtin":<String[]_value>,

"feature":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/cachepolicylabel? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "cachepolicylabel": [ { "__count": "#no"} ] }
```

cachepolicylabel_binding

Binding object which returns the resources bound to cachepolicylabel.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
labelname	<String>	Read-write	Name of the cache-policy label about which to display information.
cachepolicylabel_policybinding_binding	<cachepolicylabel_policybinding_binding[]>	Read-only	policybinding that can be bound to cachepolicylabel.
cachepolicylabel_cachepolicy_binding	<cachepolicylabel_cachepolicy_binding[]>	Read-only	cachepolicy that can be bound to cachepolicylabel.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/cachepolicylabel_binding/ labelname_value<String>

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "cachepolicylabel_binding": [ {

"labelname":<String_value>,

"cachepolicylabel_cachepolicy_binding":<cachepolicylabel_cachepolicy_binding[]_value>,

"cachepolicylabel_policybinding_binding":<cachepolicylabel_policybinding_binding[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/cachepolicylabel_binding

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters:

bulkbindings

http:// <netscaler-ip-address> /nitro/v1/config/cachepolicylabel_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "cachepolicylabel_binding": [ {

"labelname":<String_value>,

"cachepolicylabel_cachepolicy_binding":<cachepolicylabel_cachepolicy_bindi
ng[]_value>,

"cachepolicylabel_policybinding_binding":<cachepolicylabel_policybinding_b
inding[]_value>
```

```
}]}
```

cachepolicylabel_cachepolicy_binding

Binding object showing the cachepolicy that can be bound to cachepolicylabel.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
invoke_labelname	<String>	Read-write	Name of the policy label to invoke if the current policy rule evaluates to TRUE.
policyname	<String>	Read-write	Name of the cache policy to bind to the policy label.
gotopriorityexpression	<String>	Read-write	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
invoke	<Boolean>	Read-write	Invoke policies bound to a virtual server or a user-defined policy label. After the invoked policies are evaluated, the flow returns to the policy with the next-lower priority.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
labeltype	<String>	Read-write	Type of policy label to invoke: an unnamed label associated with a virtual server, or user-defined policy label. Possible values = reqvserver, resvserver, policylabel
priority	<Integer>	Read-write	Specifies the priority of the policy.
labelname	<String>	Read-write	Name of the cache policy label to which to bind the policy.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/cachepolicylabel_cachepolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"cachepolicylabel_cachepolicy_binding":{

<b>"labelname":<String_value>,

</b><b>"policyname":<String_value>,

</b><b>"priority":<Integer_value>,

</b>"gotopriorityexpression":<String_value>,
```

```
"invoke":<Boolean_value>,

"labeltype":<String_value>,

"invoke_labelname":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/cachepolicylabel_cachepolicy_binding/ labelname_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ cachepolicylabel_cachepolicy_binding/ labelname_value<String> ? **args= policyname:<String_value>, priority: <Integer_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/cachepolicylabel_cachepolicy_binding/ labelname_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ cachepolicylabel_cachepolicy_binding/ labelname_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of cachepolicylabel_cachepolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/cachepolicylabel_cachepolicy_binding/ labelname_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the cachepolicylabel_cachepolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "cachepolicylabel_cachepolicy_binding": [ {

"invoke_labelname":<String_value>,

"policyname":<String_value>,

"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"labelname":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/cachepolicylabel_cachepolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/cachepolicylabel_cachepolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "cachepolicylabel_cachepolicy_binding": [ {

"invoke_labelname":<String_value>,

"policyname":<String_value>,

"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"labelname":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/cachepolicylabel_cachepolicy_binding/ labelname_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"cachepolicylabel_cachepolicy_binding": [ { "__count": "#no"} ] }
```

cachepolicylabel_policybinding_binding

Binding object showing the policybinding that can be bound to cachepolicylabel.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
labeltype	<String>	Read-write	Type of policy label to invoke: an unnamed label associated with a virtual server, or user-defined policy label. Possible values = reqvserver,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			resvserver, policylabel
priority	<Integer>	Read-write	Specifies the priority of the policy.
labelname	<String>	Read-write	Name of the cache policy label to which to bind the policy.
gotopriorityexpression	<String>	Read-write	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
invoke	<Boolean>	Read-write	Invoke policies bound to a virtual server or a user-defined policy label. After the invoked policies are evaluated, the flow returns to the policy with the next-lower priority.
policyname	<String>	Read-write	Name of the cache policy to bind to the policy label.
invoke_labelname	<String>	Read-write	Name of the policy label to invoke if the current policy rule evaluates to TRUE.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/cachepolicylabel_policybinding_binding/ labelname_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ cachepolicylabel_policybinding_binding/ labelname_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of cachepolicylabel_policybinding_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/cachepolicylabel_policybinding_binding/ labelname_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the cachepolicylabel_policybinding_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "cachepolicylabel_policybinding_binding": [ {

"labeltype":<String_value>,

"priority":<Integer_value>,

"labelname":<String_value>,

"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>,

"policyname":<String_value>,

"invoke_labelname":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/cachepolicylabel_policybinding_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/cachepolicylabel_policybinding_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "cachepolicylabel_policybinding_binding": [ {

"labeltype":<String_value>,

"priority":<Integer_value>,

"labelname":<String_value>,

"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>,

"policyname":<String_value>,
```

```
"invoke_labelname":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/cachepolicylabel_policybinding_binding/ labelname_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"cachepolicylabel_policybinding_binding": [ { "__count": "#no"} ] }
```

cacheselector

Configuration for cache selector resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
selectorname	<String>	Read-write	Name for the selector. Must begin with an ASCII alphabetic or

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters.
rule	<String[]>	Read-write	One or multiple PIXL expressions for evaluating an HTTP request or response. Minimum length = 1
flags	<Integer>	Read-only	Flags.
builtin	<String[]>	Read-only	. Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL
feature	<String>	Read-only	The feature to be checked while applying this config.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE

- UPDATE
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/cacheselector **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"cacheselector":{

<b>"selectorname":<String_value>,

</b><b>"rule":<String[]_value>

</b>}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/cacheselector/ selectorname_value<String>
HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/cacheselector **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"cacheselector":{

<b>"selectorname":<String_value>,

</b><b>"rule":<String[]_value>
```

```
</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/cacheselector **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/cacheselector? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/cacheselector? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of cacheselector resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/cacheselector? **view=summary**

Use this query-parameter to get the summary output of cacheselector resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/cacheselector? **pagesize=#no;pageno=#no**

Use this query-parameter to get the cacheselector resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "cacheselector": [ {

"selectorname":<String_value>,

"flags":<Integer_value>,

"rule":<String[]_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/cacheselector/ selectorname_value<String>
Query-parameters: attrs http:// <netscaler-ip-address> /nitro/v1/config/cacheselector/ selectorname_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/cacheselector/ selectorname_value<String> ? **view=summary**

Use this query-parameter to get the summary output of cacheselector resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "cacheselector": [ {

"selectorname":<String_value>,

"flags":<Integer_value>,

"rule":<String[]_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/cacheselector? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "cacheselector": [ { "__count": "#no"} ] }
```

cloud

Cloud

Citrix ADC as SD proxy Configuration and cloud discovery commands.

NAME	DESCRIPTION
cloudallowedngsticketprofile	Configuration for Allowed ticket profile for NGS
cloudautoscalegroup	Configuration for Cloud autoscalegroup
cloudawsparam	Configuration for cloud awsParam
cloudcredential	Configuration for cloud credentials
cloudngsparameter	Configuration for cloud ngsparameter
cloudparameter	Configuration for cloud parameter
cloudparaminternal	Configuration for cloud paramInternal
cloudprofile	Configuration for cloud profile
cloudservice	Configuration for cloud service

NAME	DESCRIPTION
cloudvserverip	Configuration for Cloud virtual server IPs

cloudallowedngsticketprofile

Configuration for Allowed ticket profile for NGS resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Profile name for allowed tickets. Minimum length = 1
creator	<String>	Read-write	Created name for allowed tickets. Minimum length = 1
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/cloudallowedngsticketprofile **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"cloudallowedngsticketprofile":{

<b>"name":<String_value>,

</b>"creator":<String_value>
```

```
}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/cloudallowedngsticketprofile/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/cloudallowedngsticketprofile **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"cloudallowedngsticketprofile":{

<b>"name":<String_value>,

</b>"creator":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/cloudallowedngsticketprofile **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/cloudallowedngsticketprofile? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/cloudallowedngsticketprofile? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of cloudallowedngsticketprofile resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/cloudallowedngsticketprofile? **view=summary**

Use this query-parameter to get the summary output of cloudallowedngsticketprofile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/cloudallowedngsticketprofile? **pagesize=#no;pageno=#no**

Use this query-parameter to get the cloudallowedngsticketprofile resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "cloudallowedngsticketprofile": [ {

"name":<String_value>,

"creator":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/cloudallowedngsticketprofile/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/ cloudallowedngsticketprofile/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/cloudallowedngsticketprofile/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of cloudallowedngsticketprofile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "cloudallowedngsticketprofile": [ {

"name":<String_value>,

"creator":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/cloudallowedngsticketprofile? **count=yes**
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "cloudallowedngsticketprofile": [ { "__count": "#no"} ] }
```

cloudautoscalegroup

Configuration for Cloud autoscalegroup resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	.
azcount	<Integer>	Read-only	Number of Availibility Zone this Autoscale Group is in.
aznames	<String[]>	Read-only	Availibility Zones this Autoscale Group is in.
graceful	<String>	Read-only	Autoscale down policy Set for this Autoscale group. Possible values = YES, NO
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/cloudautoscalegroup **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/cloudautoscalegroup? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/cloudautoscalegroup? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of cloudautoscalegroup resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/cloudautoscalegroup? **view=summary**

Use this query-parameter to get the summary output of cloudautoscalegroup resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/cloudautoscalegroup? **pagesize=#no;pageno=#no**

Use this query-parameter to get the cloudautoscalegroup resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "cloudautoscalegroup": [ {

"name":<String_value>,

"azcount":<Integer_value>,

"aznames":<String[]_value>,

"graceful":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/cloudautoscalegroup/ name_value<String>
Query-parameters: attrs http:// <netscaler-ip-address> /nitro/v1/config/cloudautoscalegroup/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/cloudautoscalegroup/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of cloudautoscalegroup resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "cloudautoscalegroup": [ {

"name":<String_value>,

"azcount":<Integer_value>,

"aznames":<String[]_value>,

"graceful":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/cloudautoscalegroup? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "cloudautoscalegroup": [ { "__count": "#no"} ] }
```

cloudawsparam

Configuration for cloud awsParam resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
rolearn	<String>	Read-write	IAM Role ARN. Minimum length = 1
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- UPDATE
- UNSET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/cloudawsparam **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"cloudawsparam":{

"rolearn":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/cloudawsparam? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"cloudawsparam":{

"rolearn":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/cloudawsparam **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "cloudawsparam": [ {

"rolearn":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

cloudcredential

Configuration for cloud credentials resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
tenantidentifier	<String>	Read-write	Tenant ID of the Credentials. Minimum length = 1
applicationid	<String>	Read-write	Application ID of the Credentials. Minimum length = 1
applicationsecret	<String>	Read-write	Application Secret of the Credentials. Minimum length = 1
isset	<Integer>	Read-only	Are the credentials set?.
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- GET (ALL)
- UPDATE

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/cloudcredential **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"cloudcredential":{

<b>"tenantidentifier":<String_value>,

</b><b>"applicationid":<String_value>,

</b><b>"applicationsecret":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/cloudcredential **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "cloudcredential": [ {

"isset":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

cloudngsparameter

Configuration for cloud ngsparameter resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
blockonallowedngstktprof	<String>	Read-write	Enables blocking connections authenticated with a ticket createdby by an entity not whitelisted in allowedngstktprofile. Default value: NO Possible values = YES, NO
allowedudtversion	<String>	Read-write	Enables the required UDT version to EDT connections in the CGS deployment. Default value: V4 Possible values = V4, V5, V6, V7
csvserverticketingdecouple	<String>	Read-write	Enables Decoupling CSVSERVER state from Ticketing Service state in the CGS deployment. Default value: NO Possible values = YES, NO

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
allowdtls12	<String>	Read-write	Enables DTLS1.2 for client connections on CGS. Default value: NO Possible values = YES, NO
wafprotection	<String>	Read-write	Configure WAF protection for CGS deployment. The available options are: * EDGE - Edge APIs are WAF protected. * DEFAULT - NetScaler decides which endpoints have WAF protection enabled for CGS deployment. * DISABLED - WAF protection is disabled. Default value: DEFAULT Possible values = DEFAULT, DISABLED, EDGE
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- UPDATE
- UNSET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/cloudngsparameter **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"cloudngsparameter":{

"blockonallowedngstktprof":<String_value>,

"allowedudtversion":<String_value>,

"csvserverticketingdecouple":<String_value>,

"allowdtls12":<String_value>,

"wafprotection":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/cloudngsparameter? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"cloudngsparameter":{

"blockonallowedngstktprof":true,

"allowedudtversion":true,

"csvserverticketingdecouple":true,

"allowdtls12":true,

"wafprotection":true
```

```
}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/cloudngsparameter **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "cloudngsparameter": [ {

"blockonallowedngstktprof":<String_value>,

"allowedudtversion":<String_value>,

"csvserverticketingdecouple":<String_value>,

"allowdtls12":<String_value>,

"wafprotection":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

cloudparameter

Configuration for cloud parameter resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
controllerfqdn	<String>	Read-write	FQDN of the controller to which the Citrix ADC SDProxy Connects. Minimum length = 1
controllerport	<Integer>	Read-write	Port number of the controller to which the Citrix ADC SDProxy connects. Minimum value = 1 Range 1 - 65535 * in CLI is represented as 65535 in NITRO API
instanceid	<String>	Read-write	Instance ID of the customer provided by Trust. Minimum length = 1
customerid	<String>	Read-write	Customer ID of the citrix cloud customer. Minimum length = 1
resourcelocation	<String>	Read-write	Resource Location of the customer provided by Trust.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum length = 1
activationcode	<String>	Read-write	Activation code for the NGS Connector instance.
deployment	<String>	Read-write	Describes if the customer is a Staging/Production or Dev Citrix Cloud customer. Possible values = Production, Staging, Dev
connectorresidence	<String>	Read-write	Identifies whether the connector is located Onprem, Aws or Azure. Possible values = None, Onprem, Aws, Azure, Cpx
controlconnectionstatus	<String>	Read-only	Status of the control connection: In case of successful registration to the controller, connection status will be shown as "Registered" else "Unregistered".
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- UPDATE
- UNSET

- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/cloudparameter **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"cloudparameter":{

"controllerfqdn":<String_value>,
```

```
"controllerport":<Integer_value>,

"instanceid":<String_value>,

"customerid":<String_value>,

"resourcelocation":<String_value>,

"activationcode":<String_value>,

"deployment":<String_value>,

"connectorresidence":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/cloudparameter? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"cloudparameter":{

"instanceid":true,

"customerid":true,

"resourcelocation":true
```

```
}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/cloudparameter **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "cloudparameter": [ {

"controllerfqdn":<String_value>,

"controllerport":<Integer_value>,

"instanceid":<String_value>,

"customerid":<String_value>,

"resourcelocation":<String_value>,

"controlconnectionstatus":<String_value>,

"deployment":<String_value>,
```

```
"connectorresidence":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

cloudparaminternal

Configuration for cloud paramInternal resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
nonftumode	<String>	Read-write	Indicates if GUI in in FTU mode or not. Possible values = YES, NO
iamperm	<String>	Read-only	Indicates if user has sufficient IAM previliges. Default value: NO Possible values = YES, NO
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET (ALL)
- COUNT
- UPDATE

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/cloudparaminternal **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"cloudparaminternal":{

"nonftumode":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/cloudparaminternal **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/cloudparaminternal? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/cloudparaminternal? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of cloudparaminternal resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/cloudparaminternal? **view=summary**

Use this query-parameter to get the summary output of cloudparaminternal resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/cloudparaminternal? **pagesize=#no;pageno=#no**

Use this query-parameter to get the cloudparaminternal resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "cloudparaminternal": [ {

"nonftumode":<String_value>,

"iamperm":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/cloudparaminternal? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "cloudparaminternal": [ { "__count": "#no"} ] }
```

cloudprofile

Configuration for cloud profile resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the Cloud profile. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the profile is created. Minimum length = 1 Maximum length = 127
type	<String>	Read-write	Type of cloud profile that you want to create, Vserver or based on Azure Tags. Possible values = autoscale, azuretags
vservername	<String>	Read-write	Name for the virtual server. Must begin with an ASCII alphanumeric or

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at sign (@), equal sign (=), and hyphen (-) characters. Can be changed after the virtual server is created. CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my vserver" or 'my vserver'). . Minimum length = 1
servicetype	<String>	Read-write	Protocol used by the service (also called the service type). Possible values = HTTP, FTP, TCP, UDP, SSL, SSL_BRIDGE, SSL_TCP, DTLS, NNTP, DNS, DHCPRA, ANY, SIP_UDP, SIP_TCP, SIP_SSL, DNS_TCP, RTSP,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			PUSH, SSL_PUSH, RADIUS, RDP, MYSQL, MSSQL, DIAMETER, SSL_DIAMETER, TFTP, ORACLE, SMPP, SYSLOGTCP, SYSLOGUDP, FIX, SSL_FIX, PROXY, USER_TCP, USER_SSL_TCP, QUIC, IPFIX, LOGSTREAM, MONGO, MONGO_TLS, MQTT, MQTT_TLS, QUIC_BRIDGE, HTTP_QUIC, DOT, SSL_PROXY, KAFKA_PRODUCER
ipaddress	<String>	Read-write	IPv4 or IPv6 address to assign to the virtual server.
port	<Integer>	Read-write	Port number for the virtual server. Range 1 - 65535 * in CLI is represented as 65535 in NITRO API

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
servicegroupname	<String>	Read-write	servicegroups bind to this server.
boundservicegroups vctype	<String>	Read-write	The type of bound service. Possible values = HTTP, FTP, TCP, UDP, SSL, SSL_BRIDGE, SSL_TCP, DTLS, NNTP, RPCSVR, DNS, ADNS, SNMP, RTSP, DHCPRA, ANY, SIP_UDP, SIP_TCP, SIP_SSL, DNS_TCP, ADNS_TCP, MYSQL, MSSQL, ORACLE, MONGO, MONGO_TLS, RADIUS, RADIUSListener, RDP, DIAMETER, SSL_DIAMETER, TFTP, SMPP, PPTP, GRE, SYSLOGTCP, SYSLOGUDP, FIX, SSL_FIX, USER_TCP, USER_SSL_TCP, QUIC, IPFIX, LOGSTREAM, LOGSTREAM_SSL, MQTT, MQTT_TLS, QUIC_BRIDGE, DOT, ADNS_DOT,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			HTTP_QUIC, ADNS_DOH, KAFKA_BROKER
vsvrbindsvcport	<Integer>	Read-write	The port number to be used for the bound service. Range 1 - 65535 * in CLI is represented as 65535 in NITRO API
graceful	<String>	Read-write	Indicates graceful shutdown of the service. System will wait for all outstanding connections to this service to be closed before disabling the service. Default value: NO Possible values = YES, NO
delay	<Integer>	Read-write	Time, in seconds, after which all the services configured on the server are disabled.
azuretagname	<String>	Read-write	Azure tag name. Maximum length = 512
azuretagvalue	<String>	Read-write	Azure tag value.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum length = 256
azurepollperiod	<Integer>	Read-write	Azure polling period (in seconds). Default value: 60 Minimum value = 60 Maximum value = 3600
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of

creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/cloudprofile **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"cloudprofile":{

<b>"name":<String_value>,

</b><b>"type":<String_value>,

</b><b>"vservername":<String_value>,

</b><b>"servicetype":<String_value>,

</b><b>"ipaddress":<String_value>,

</b><b>"port":<Integer_value>,

</b><b>"servicegroupname":<String_value>,

</b><b>"boundservicegroupsvctype":<String_value>,
```

```
</b><b>"vsvrbindsvcport":<Integer_value>,

</b>"graceful":<String_value>,

"delay":<Integer_value>,

"azuretagname":<String_value>,

"azuretagvalue":<String_value>,

"azurepollperiod":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/cloudprofile/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/cloudprofile **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/cloudprofile? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/cloudprofile? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of cloudprofile resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/cloudprofile? **view=summary**

Use this query-parameter to get the summary output of cloudprofile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/cloudprofile? **pagesize=#no;pageno=#no**

Use this query-parameter to get the cloudprofile resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "cloudprofile": [ {

"name":<String_value>,

"type":<String_value>,

"vservername":<String_value>,

"servicetype":<String_value>,

"ipaddress":<String_value>,
```

```
"port":<Integer_value>,

"servicegroupname":<String_value>,

"boundservicegroupsvctype":<String_value>,

"vsvrbindsvcport":<Integer_value>,

"azuretagname":<String_value>,

"azuretagvalue":<String_value>,

"azurepollperiod":<Integer_value>,

"graceful":<String_value>,

"delay":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/cloudprofile/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/cloudprofile/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/cloudprofile/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of cloudprofile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "cloudprofile": [ {

"name":<String_value>,

"type":<String_value>,

"vservername":<String_value>,

"servicetype":<String_value>,

"ipaddress":<String_value>,

"port":<Integer_value>,

"servicegroupname":<String_value>,

"boundservicegroupsvctype":<String_value>,

"vsvrbindsvcport":<Integer_value>,

"azuretagname":<String_value>,

"azuretagvalue":<String_value>,

"azurepollperiod":<Integer_value>,

"graceful":<String_value>,

"delay":<Integer_value>,
```

```
"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/cloudprofile? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "cloudprofile": [ { "__count": "#no"} ] }
```

cloudservice

Configuration for cloud service resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
response	<String>	Read-write	.

Operations

(click to see Properties)

- CHECK

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

CHECK

URL: http:// <netscaler-ip-address> /nitro/v1/config/cloudservice? **action=check**

HTTP Method: POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"cloudservice":{

}}
```

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Payload:

```
{ "cloudservice": [ {

"response":<String_value>



}]}
```

cloudvserverip

Configuration for Cloud virtual server IPs resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ipaddress	<String>	Read-write	VIPS on a given ENI.
_nextgenapiresource	<String>	Read-write	.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/cloudvserverip

Query-parameters:

attrs

http:// <netscaler-ip-address> /nitro/v1/config/cloudvserverip? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter

http:// <netscaler-ip-address> /nitro/v1/config/cloudvserverip? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of cloudvserverip resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view

http:// <netscaler-ip-address> /nitro/v1/config/cloudvserverip? **view=summary**

Use this query-parameter to get the summary output of cloudvserverip resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination

http:// <netscaler-ip-address> /nitro/v1/config/cloudvserverip? **pagesize=#no;pageno=#no**

Use this query-parameter to get the cloudvserverip resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "cloudvserverip": [ {

"ipaddress":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/cloudvserverip? **count=yes**

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "cloudvserverip": [ { "__count": "#no"} ] }
```

cloudtunnel

Cloudtunnel

Cloudtunnel Virtual server configuration.

NAME	DESCRIPTION
cloudtunnelparameter	Configuration for Cloudtunnel parameter
cloudtunnelvserver	Configuration for Cloud Tunnel virtual server

cloudtunnelparameter

Configuration for Cloudtunnel parameter resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
controllerfqdn	<String>	Read-write	.
fqdn	<String>	Read-write	.
resourcelocation	<String>	Read-write	.
subnetresourcelocationmappings	<String>	Read-write	.
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- UPDATE
- UNSET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/cloudtunnelparameter

HTTP Method: PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"cloudtunnelparameter":{

"controllerfqdn":<String_value>,

"fqdn":<String_value>,
```

```
"resourcelocation":<String_value>,

"subnetresourcelocationmappings":<String_value>

}}
```

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/cloudtunnelparameter? **action=unset**

HTTP Method: POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"cloudtunnelparameter":{

"subnetresourcelocationmappings":true

}}
```

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/cloudtunnelparameter

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "cloudtunnelparameter": [ {

"controllerfqdn":<String_value>,

"fqdn":<String_value>,

"resourcelocation":<String_value>,

"subnetresourcelocationmappings":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

cloudtunnelvserver

Configuration for Cloud Tunnel virtual server resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the Cloud Tunnel virtual server. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space,colon (:), at (@), equals (=), and hyphen (-) characters. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my server" or 'my server'). Minimum length = 1
servicetype	<String>	Read-write	ServiceType of Listener using which

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			traffic will be tunneled through cloud tunnel server. Possible values = TCP, UDP
listenpolicy	<String>	Read-write	String specifying the listen policy for the Cloud Tunnel virtual server. Can be either a named expression or an expression. The Cloud Tunnel virtual server processes only the traffic for which the expression evaluates to true. Default value: "none"
listenpriority	<Integer>	Read-write	Integer specifying the priority of the listen policy. A higher number specifies a lower priority. If a request matches the listen policies of more than one virtual server, the virtual server whose listen policy has the highest priority (the lowest priority number) accepts the request. Default value: 101 Minimum value = 0

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum value = 100
state	<String>	Read-only	The current state of the virtual server, as UP, DOWN, BUSY, and so on. Possible values = UP, DOWN, UNKNOWN, BUSY, OUT OF SERVICE, GOING OUT OF SERVICE, DOWN WHEN GOING OUT OF SERVICE, NS_EMPTY_STR, Unknown, DISABLED
effectivestate	<String>	Read-only	. Possible values = UP, DOWN, UNKNOWN, BUSY, OUT OF SERVICE, GOING OUT OF SERVICE, DOWN WHEN GOING OUT OF SERVICE, NS_EMPTY_STR, Unknown, DISABLED
type	<String>	Read-only	The type of virtual server; for example, CONTENT based or ADDRESS based.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = CONTENT, ADDRESS
ip	<String>	Read-only	The Virtual IP address of the Cloud Tunnel virtual server.
ipv46	<String>	Read-only	IPv4 or IPv6 address of the Cloud Tunnel virtual server. Minimum length = 1
ippattern	<String>	Read-only	The IP pattern of the virtual server.
port	<Integer>	Read-only	Port on which the virtual server listens. Range 1 - 65535 * in CLI is represented as 65535 in NITRO API
range	<Integer>	Read-only	. Default value: 1 Minimum value = 1 Maximum value = 254
cachetype	<String>	Read-only	Virtual server cache type. The options are: TRANSPARENT, REVERSE, and FORWARD.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = TRANSPARENT, REVERSE, FORWARD
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET (ALL)
- GET
- COUNT
- UPDATE

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/cloudtunnelvserver **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"cloudtunnelvserver":{

<b>"name":<String_value>,

</b><b>"servicetype":<String_value>,

</b>"listenpolicy":<String_value>,

"listenpriority":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/cloudtunnelvserver/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/cloudtunnelvserver **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"cloudtunnelvserver":{

<b>"name":<String_value>,

</b>"listenpolicy":<String_value>,

"listenpriority":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/cloudtunnelvserver **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/cloudtunnelvserver? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/cloudtunnelvserver? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of cloudtunnelvserver resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/cloudtunnelvserver? **view=summary**

Use this query-parameter to get the summary output of cloudtunnelvserver resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/cloudtunnelvserver? **pagesize=#no;pageno=#no**

Use this query-parameter to get the cloudtunnelvserver resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "cloudtunnelvserver": [ {

"name":<String_value>,

"servicetype":<String_value>,

"state":<String_value>,

"effectivestate":<String_value>,

"type":<String_value>,
```

```
"ip":<String_value>,

"ipv46":<String_value>,

"ippattern":<String_value>,

"port":<Integer_value>,

"range":<Integer_value>,

"cachetype":<String_value>,

"listenpolicy":<String_value>,

"listenpriority":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/cloudtunnelvserver/ name_value<String>
Query-parameters: attrs http:// <netscaler-ip-address> /nitro/v1/config/cloudtunnelvserver/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/cloudtunnelvserver/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of cloudtunnelvserver resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "cloudtunnelvserver": [ {

"name":<String_value>,

"servicetype":<String_value>,

"state":<String_value>,

"effectivestate":<String_value>,

"type":<String_value>,

"ip":<String_value>,

"ipv46":<String_value>,

"ippattern":<String_value>,

"port":<Integer_value>,

"range":<Integer_value>,

"cachetype":<String_value>,

"listenpolicy":<String_value>,

"listenpriority":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

```
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/cloudtunnelvserver? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "cloudtunnelvserver": [ { "__count": "#no"} ] }
```

cluster

Cluster

Cluster commands.

NAME	DESCRIPTION
cluster	
clusterfiles	Configuration for files
clusterinstance	Configuration for cluster instance
clusterinstance_binding	Binding object showing the resources that can be bound to clusterinstance

NAME	DESCRIPTION
clusterinstance_clusternode_binding	Binding object showing the clusternode that can be bound to clusterinstance
clusternode	Configuration for cluster node
clusternode_binding	Binding object showing the resources that can be bound to clusternode
clusternode_routemonitor_binding	Binding object showing the routemonitor that can be bound to clusternode
clusternodegroup	Configuration for Node group object type
clusternodegroup_authenticationvserver_binding	Binding object showing the authenticationvserver that can be bound to clusternodegroup
clusternodegroup_binding	Binding object showing the resources that can be bound to clusternodegroup
clusternodegroup_clusternode_binding	Binding object showing the clusternode that can be bound to clusternodegroup
clusternodegroup_crvserver_binding	Binding object showing the crvserver that can be bound to clusternodegroup
clusternodegroup_csvserver_binding	Binding object showing the csvserver that can be bound to clusternodegroup
clusternodegroup_gslbsite_binding	Binding object showing the gslbsite that can be bound to clusternodegroup
clusternodegroup_gslbvserver_binding	Binding object showing the gslbvserver that can be bound to clusternodegroup
clusternodegroup_lbvserver_binding	Binding object showing the lbvserver that can be bound to clusternodegroup

NAME	DESCRIPTION
clusternodegroup_nslimitidentifier_binding	Binding object showing the nslimitidentifier that can be bound to clusternodegroup
clusternodegroup_service_binding	Binding object showing the service that can be bound to clusternodegroup
clusternodegroup_streamidentifier_binding	Binding object showing the streamidentifier that can be bound to clusternodegroup
clusternodegroup_vpnvserver_binding	Binding object showing the vpnvserver that can be bound to clusternodegroup
clusterpropstatus	
clustersync	Configuration for sync
clustersyncfailures	Configuration for Cluster sync failures

cluster

Configuration for 0 resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
clip	<String>	Read-write	Cluster IP address to which to add the node.
password	<String>	Read-write	Password for the nsroot account of the configuration coordinator (CCO).

Operations

(click to see Properties)

- JOIN

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

JOIN

URL: http:// <netscaler-ip-address> /nitro/v1/config/cluster? **action=join**

HTTP Method: POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"cluster":{

<b>"clip":<String_value>,

</b><b>"password":<String_value>

</b>}}
```

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

clusterfiles

Configuration for files resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
mode	<String[]>	Read-write	The directories and files to be synchronized. The available settings function as follows: Mode Paths all /nsconfig/ssl/ /var/netscaler/ssl/ /var/vpn/bookmark/ /nsconfig/dns/

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			/nsconfig/monitors/ /nsconfig/nstemplates/ /nsconfig/ssh/ /nsconfig/rc.netscaler /nsconfig/resolv.conf /nsconfig/inetd.conf /nsconfig/syslog.conf /nsconfig/ntp.conf /nsconfig/httpd.conf /nsconfig/sshd_config /nsconfig/hosts /nsconfig/enckey /var/nslw.bin/etc/krb5.conf /var/nslw.bin/etc/krb5.keytab /var/lib/likewise/db/ /var/download/ /var/wi/tomcat/webapps/

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			/var/wi/tomcat/conf/Catalina/localhost/ /var/wi/java_home/lib/security/cacerts /var/wi/java_home/jre/lib/security/cacerts /var/netscaler/locdb/ ssl /nsconfig/ssl/ /var/netscaler/ssl/ bookmarks /var/vpn/bookmark/ dns /nsconfig/dns/ imports /var/download/ misc /nsconfig/license/ /nsconfig/rc.conf all_plus_misc Includes *all* files and /nsconfig/license/ and /nsconfig/rc.conf. Default value: all. Possible values = all, bookmarks, ssl, imports, misc, dns, krb, AAA,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			app_catalog, all_plus_misc, all_minus_misc

Operations

(click to see Properties)

- SYNC

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

SYNC

URL: http:// <netscaler-ip-address> /nitro/v1/config/clusterfiles? **action=sync HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"clusterfiles":{

"mode":<String[]_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

clusterinstance

Configuration for cluster instance resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
clid	<Integer>	Read-write	Unique number that identifies the cluster. Minimum value = 1 Maximum value = 128
deadinterval	<Integer>	Read-write	Amount of time, in seconds, after which nodes that do not respond to the heartbeats are assumed to be down.If the value is

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			less than 3 sec, set the helloInterval parameter to 200 msec. Default value: 3 Minimum value = 1 Maximum value = 60
hellointerval	<Integer>	Read-write	Interval, in milliseconds, at which heartbeats are sent to each cluster node to check the health status.Set the value to 200 msec, if the deadInterval parameter is less than 3 sec. Default value: 200 Minimum value = 200 Maximum value = 1000
preemption	<String>	Read-write	Preempt a cluster node that is configured as a SPARE if an ACTIVE node becomes available. Default value: DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ENABLED, DISABLED
quorumtype	<String>	Read-write	Quorum Configuration Choices - "Majority" (recommended) requires majority of nodes to be online for the cluster to be UP. "None" relaxes this requirement. Default value: MAJORITY Possible values = MAJORITY, NONE
inc	<String>	Read-write	This option is required if the cluster nodes reside on different networks. Default value: DISABLED Possible values = ENABLED, DISABLED
processlocal	<String>	Read-write	By turning on this option packets destined to a service in a cluster will not under go any steering. Default value: DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ENABLED, DISABLED
retainconnectionsoncluster	<String>	Read-write	This option enables you to retain existing connections on a node joining a Cluster system or when a node is being configured for passive timeout. By default, this option is disabled. Default value: NO Possible values = YES, NO
backplanebasedview	<String>	Read-write	View based on heartbeat only on bkplane interface. Default value: DISABLED Possible values = ENABLED, DISABLED
syncstatusstrictmode	<String>	Read-write	strict mode for sync status of cluster. Depending on the the mode if there are any errors while applying config, sync status is displayed accordingly. By default the flag is disabled.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: DISABLED Possible values = ENABLED, DISABLED
dfdretainl2params	<String>	Read-write	flag to add ext l2 header during steering. By default the flag is disabled. Default value: DISABLED Possible values = ENABLED, DISABLED
clusterproxyarp	<String>	Read-write	This field controls the proxy arp feature in cluster. By default the flag is enabled. Default value: ENABLED Possible values = ENABLED, DISABLED
secureheartbeats	<String>	Read-write	By turning on this option cluster heartbeats will have security enabled. Default value: DISABLED Possible values = ENABLED, DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
nodegroup	<String>	Read-write	The node group in a Cluster system used for transition from L2 to L3.
adminstate	<String>	Read-only	Cluster Admin State. Default value: DISABLED Possible values = ENABLED, DISABLED
propstate	<String>	Read-only	Enable/Disable the execution of commands on the cluster. This will not impact the execution of commands on individual cluster nodes by using the NSIP. Default value: ENABLED Possible values = ENABLED, DISABLED
validmtu	<Integer>	Read-only	Correct MTU value that has to be set on backplane.
heterogeneousflag	<String>	Read-only	This field diplay if heterogeneous is detected in the cluster system. Default value: NO

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = YES, NO
operationalstate	<String>	Read-only	Cluster Operational State. Possible values = ENABLED, DISABLED
status	<String>	Read-only	Cluster Operational State. Possible values = DOWN, UP, PARTIAL-UP, UNKNOWN
rsskeymismatch	<Boolean>	Read-only	This argument is used to determine if there is a RSS key mismatch at cluster instance level.
penummismatch	<Boolean>	Read-only	This argument is used to determine if there is a PE number mismatch at cluster instance level.
nodegroupstatewarning	<Boolean>	Read-only	This argumnt is used to determind whether all the cluster nodes are bound to nodegroup with state set.
licensemismatch	<Boolean>	Read-only	This argument is used to determine if there is a License mismatch at cluster instance level.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
jumbonotsupported	<Boolean>	Read-only	This argument is used to determine if Jumbo framework is not supported at cluster instance level.
clustertunnelmodemismatch	<Boolean>	Read-only	This argument is used to determine if different tunnel mode configured on cluster nodes.
clusternoheartbeatonnode	<Boolean>	Read-only	HB is not seen on the backplane interface of member node.
clusternolinksetmbf	<Boolean>	Read-only	MBF is enabled but linkset is not configured .
clusternospottedip	<Boolean>	Read-only	There is no spotted SNIP or MIP.
clusterclipfailure	<Boolean>	Read-only	CLIP movement failure. CLIP is not attached to CCO.
clusterhbhmacerrordetected	<Boolean>	Read-only	There is cluster hb hmac error detected, it could be due to version mismatch.
nodepenummismatch	<Boolean>	Read-only	This argument is used to determine if there is a PE mismatch at cluster node level.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
operationalpropstate	<String>	Read-only	Cluster Operational Propagation State. Default value: ENABLED Possible values = UNKNOWN, ENABLED, DISABLED, AUTO DISABLED, AUTO DISABLED (Disk Encryption Mismatch)
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- ENABLE
- DISABLE
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/clusterinstance **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"clusterinstance":{

<b>"clid":<Integer_value>,

</b>"deadinterval":<Integer_value>,

"hellointerval":<Integer_value>,

"preemption":<String_value>,

"quorumtype":<String_value>,
```

```
"inc":<String_value>,

"processlocal":<String_value>,

"retainconnectionsoncluster":<String_value>,

"backplanebasedview":<String_value>,

"syncstatusstrictmode":<String_value>,

"dfdretainl2params":<String_value>,

"clusterproxyarp":<String_value>,

"secureheartbeats":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/clusterinstance/ clid_value<Integer> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/clusterinstance **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"clusterinstance":{

<b>"clid":<Integer_value>,

</b>"deadinterval":<Integer_value>,

"hellointerval":<Integer_value>,

"preemption":<String_value>,

"quorumtype":<String_value>,

"inc":<String_value>,

"processlocal":<String_value>,

"nodegroup":<String_value>,

"retainconnectionsoncluster":<String_value>,

"backplanebasedview":<String_value>,

"syncstatusstrictmode":<String_value>,

"dfdretainl2params":<String_value>,

"clusterproxyarp":<String_value>,

"secureheartbeats":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/clusterinstance? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"clusterinstance":{

<b>"clid":<Integer_value>,

</b>"deadinterval":true,

"hellointerval":true,

"preemption":true,

"quorumtype":true,

"inc":true,

"processlocal":true,

"nodegroup":true,

"retainconnectionsoncluster":true,

"backplanebasedview":true,

"syncstatusstrictmode":true,

"dfdretainl2params":true,

"clusterproxyarp":true,

"secureheartbeats":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

ENABLE

URL: http:// <netscaler-ip-address> /nitro/v1/config/clusterinstance? **action=enable HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"clusterinstance":{

<b>"clid":<Integer_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DISABLE

URL: http:// <netscaler-ip-address> /nitro/v1/config/clusterinstance? **action=disable HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"clusterinstance":{

<b>"clid":<Integer_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/clusterinstance **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/clusterinstance? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/clusterinstance? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of clusterinstance resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/clusterinstance? **view=summary**

Use this query-parameter to get the summary output of clusterinstance resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/clusterinstance? **pagesize=#no;pageno=#no**

Use this query-parameter to get the clusterinstance resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "clusterinstance": [ {

"clid":<Integer_value>,

"deadinterval":<Integer_value>,

"hellointerval":<Integer_value>,

"preemption":<String_value>,

"adminstate":<String_value>,

"quorumtype":<String_value>,

"propstate":<String_value>,

"inc":<String_value>,

"nodegroup":<String_value>,

"processlocal":<String_value>,

"validmtu":<Integer_value>,

"retainconnectionsoncluster":<String_value>,

"heterogeneousflag":<String_value>,

"backplanebasedview":<String_value>,

"syncstatusstrictmode":<String_value>,

"dfdretainl2params":<String_value>,
```

```
"clusterproxyarp":<String_value>,

"secureheartbeats":<String_value>,

"operationalstate":<String_value>,

"status":<String_value>,

"rsskeymismatch":<Boolean_value>,

"penummismatch":<Boolean_value>,

"nodegroupstatewarning":<Boolean_value>,

"licensemismatch":<Boolean_value>,

"jumbonotsupported":<Boolean_value>,

"clustertunnelmodemismatch":<Boolean_value>,

"clusternoheartbeatonnode":<Boolean_value>,

"clusternolinksetmbf":<Boolean_value>,

"clusternospottedip":<Boolean_value>,

"clusterclipfailure":<Boolean_value>,

"clusterhbhmacerrordetected":<Boolean_value>,

"nodepenummismatch":<Boolean_value>,

"operationalpropstate":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/clusterinstance/ clid_value<Integer> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/clusterinstance/ clid_value<Integer> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/clusterinstance/ clid_value<Integer> ? **view=summary**

Use this query-parameter to get the summary output of clusterinstance resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "clusterinstance": [ {

"clid":<Integer_value>,

"deadinterval":<Integer_value>,

"hellointerval":<Integer_value>,

"preemption":<String_value>,
```

```
"adminstate":<String_value>,

"quorumtype":<String_value>,

"propstate":<String_value>,

"inc":<String_value>,

"nodegroup":<String_value>,

"processlocal":<String_value>,

"validmtu":<Integer_value>,

"retainconnectionsoncluster":<String_value>,

"heterogeneousflag":<String_value>,

"backplanebasedview":<String_value>,

"syncstatusstrictmode":<String_value>,

"dfdretainl2params":<String_value>,

"clusterproxyarp":<String_value>,

"secureheartbeats":<String_value>,

"operationalstate":<String_value>,

"status":<String_value>,

"rsskeymismatch":<Boolean_value>,

"penummismatch":<Boolean_value>,

"nodegroupstatewarning":<Boolean_value>,

"licensemismatch":<Boolean_value>,

"jumbonotsupported":<Boolean_value>,

"clustertunnelmodemismatch":<Boolean_value>,
```

```
"clusternoheartbeatonnode":<Boolean_value>,

"clusternolinksetmbf":<Boolean_value>,

"clusternospottedip":<Boolean_value>,

"clusterclipfailure":<Boolean_value>,

"clusterhbhmacerrordetected":<Boolean_value>,

"nodepenummismatch":<Boolean_value>,

"operationalpropstate":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/clusterinstance? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "clusterinstance": [ { "__count": "#no"} ] }
```

clusterinstance_binding

Binding object which returns the resources bound to clusterinstance.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
clid	<Integer>	Read-write	Unique number that identifies the cluster. Minimum value = 1 Maximum value = 128
clusterinstance_clusternode_binding	<clusterinstance_clusternode_binding[]>	Read-only	clusternode that can be bound to clusterinstance.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.
- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/clusterinstance_binding/ clid_value<Integer>
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "clusterinstance_binding": [ {

"clid":<Integer_value>,

"clusterinstance_clusternode_binding":<clusterinstance_clusternode_binding
[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/clusterinstance_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/clusterinstance_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "clusterinstance_binding": [ {

"clid":<Integer_value>,

"clusterinstance_clusternode_binding":<clusterinstance_clusternode_binding
[]_value>

}]}
```

clusterinstance_clusternode_binding

Binding object showing the clusternode that can be bound to clusterinstance.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
nodeid	<Integer>	Read-write	The unique number that identiies a cluster. Minimum value = 0 Maximum value = 31
clid	<Integer>	Read-write	Unique number that identifies the cluster. Minimum value = 1 Maximum value = 128
health	<String>	Read-only	Node Health state. Possible values = UNKNOWN, INIT, DOWN, UP, Some enabled and HAMON interfaces of the node are down, All interfaces of the node are down or disabled, SSL card(s) of the node have failed, Route Monitor(s) of the node have failed, Service state is being synchronized with the cluster, The backplane interface is either not set or it is down or is disabled, The CLAG

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			member(s) of the node are down, Persistence sessions are being synchronized with the cluster, The Syn Cookie is being synchronized with the cluster, Unknown Health, AAA keys are being sychronized with the cluster, Cluster health is not up due to config sync is in progress
clusterhealth	<String>	Read-only	Node clusterd state. Possible values = UP, Configurations of the node are lagging behind the cluster by more than 256 commands, The config sync operation has exceeded the time limit of 60 seconds, The config sync operation (full sync) is in progress, The node is not in sync with the cluster configurations as sync is disabled on

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			this node, The execution of a configuration command has failed on this node, UNKNOWN
state	<String>	Read-only	Active, Spare or Passive. An active node serves traffic. A spare node serves as a backup for active nodes. A passive node does not serve traffic. This may be useful during temporary maintenance activity where it is desirable that the node takes part in the consensus protocol, but not serve traffic. Default value: PASSIVE Possible values = ACTIVE, SPARE, PASSIVE
nodelicensemismatch	<Boolean>	Read-only	This argument is used to determine if there is a License mismatch at cluster node level.
islocalnode	<Boolean>	Read-only	This argument is used to determine whether it is local node.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ipaddress	<String>	Read-only	The IP Address of the node.
nodejumbonotsupported	<Boolean>	Read-only	This argument is used to determine if Jumbo framework not supported at cluster node level.
masterstate	<String>	Read-only	Master state. Possible values = INACTIVE, ACTIVE, UNKNOWN
isconfigurationcoordinator	<Boolean>	Read-only	This argument is used to determine whether the node is configuration coordinator (CCO).
nodersskeymismatch	<Boolean>	Read-only	This argument is used to determine if there is a RSS key mismatch at cluster node level.
effectivestate	<String>	Read-only	Node effective health state. Possible values = UP, NOT UP, UNKNOWN, INIT
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)

- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/clusterinstance_clusternode_binding/ clid_value<Integer> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ clusterinstance_clusternode_binding/ clid_value<Integer> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of clusterinstance_clusternode_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/clusterinstance_clusternode_binding/ clid_value<Integer> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the clusterinstance_clusternode_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "clusterinstance_clusternode_binding": [ {

"nodeid":<Integer_value>,

"clid":<Integer_value>,

"health":<String_value>,

"clusterhealth":<String_value>,

"state":<String_value>,

"nodelicensemismatch":<Boolean_value>,

"islocalnode":<Boolean_value>,

"ipaddress":<String_value>,

"nodejumbonotsupported":<Boolean_value>,

"masterstate":<String_value>,

"isconfigurationcoordinator":<Boolean_value>,

"nodersskeymismatch":<Boolean_value>,
```

```
"effectivestate":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/clusterinstance_clusternode_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/clusterinstance_clusternode_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "clusterinstance_clusternode_binding": [ {

"nodeid":<Integer_value>,

"clid":<Integer_value>,

"health":<String_value>,

"clusterhealth":<String_value>,
```

```
"state":<String_value>,

"nodelicensemismatch":<Boolean_value>,

"islocalnode":<Boolean_value>,

"ipaddress":<String_value>,

"nodejumbonotsupported":<Boolean_value>,

"masterstate":<String_value>,

"isconfigurationcoordinator":<Boolean_value>,

"nodersskeymismatch":<Boolean_value>,

"effectivestate":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/clusterinstance_clusternode_binding/clid_value<Integer> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"clusterinstance_clusternode_binding": [ { "__count": "#no"} ] }
```

clusternode

Configuration for cluster node resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
nodeid	<Integer>	Read-write	Unique number that identifies the cluster node. Minimum value = 0 Maximum value = 31
ipaddress	<String>	Read-write	Citrix ADC IP (NSIP) address of the appliance to add to the cluster. Must be an IPv4 address. Minimum length = 1
state	<String>	Read-write	Admin state of the cluster node. The available settings function as follows: ACTIVE - The node serves traffic. SPARE - The node does not serve traffic unless an ACTIVE node goes down.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			PASSIVE - The node does not serve traffic, unless you change its state. PASSIVE state is useful during temporary maintenance activities in which you want the node to take part in the consensus protocol but not to serve traffic. Default value: PASSIVE Possible values = ACTIVE, SPARE, PASSIVE
backplane	<String>	Read-write	Interface through which the node communicates with the other nodes in the cluster. Must be specified in the three-tuple form n/c/u, where n represents the node ID and c/u refers to the interface on the appliance. Minimum length = 1
priority	<Integer>	Read-write	Preference for selecting a node as the configuration

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			coordinator. The node with the lowest priority value is selected as the configuration coordinator. When the current configuration coordinator goes down, the node with the next lowest priority is made the new configuration coordinator. When the original node comes back up, it will preempt the new configuration coordinator and take over as the configuration coordinator. Note: When priority is not configured for any of the nodes or if multiple nodes have the same priority, the cluster elects one of the nodes as the configuration coordinator. Default value: 31 Minimum value = 0

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum value = 31
nodegroup	<String>	Read-write	The default node group in a Cluster system. Default value: DEFAULT_NG Minimum length = 1
delay	<Integer>	Read-write	Applicable for Passive node and node becomes passive after this timeout (in minutes). Default value: 0 Minimum value = 0 Maximum value = 1440
tunnelmode	<String>	Read-write	To set the tunnel mode. Default value: NONE Possible values = NONE, GRE, UDP
clearnodegroupconfig	<String>	Read-write	Option to remove nodegroup config. Default value: YES Possible values = YES, NO
force	<Boolean>	Read-write	Node will be removed from cluster

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			without prompting for user confirmation.
clusterhealth	<String>	Read-only	Node clusterd state. Possible values = UP, Configurations of the node are lagging behind the cluster by more than 256 commands, The config sync operation has exceeded the time limit of 60 seconds, The config sync operation (full sync) is in progress, The node is not in sync with the cluster configurations as sync is disabled on this node, The execution of a configuration command has failed on this node, UNKNOWN
effectivestate	<String>	Read-only	Node effective health state. Possible values = UP, NOT UP, UNKNOWN, INIT
operationalsyncstate	<String>	Read-only	Node Operational Reconciliation state.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: ENABLED Possible values = ENABLED, SUCCESS, IN PROGRESS, PARTIAL SUCCESS, FAILED, INCREMENTAL SYNC DISABLED, DISABLED, UNKNOWN
syncfailurereason	<String>	Read-only	Displays the additional information along with cluster sync status. Possible values = Refer the files clus_sync_batch_status.log, sync_route_status.log and sync_clusdiff_status.log in /var/nssynclog directory for list of commands failed
masterstate	<String>	Read-only	Node Master state. Possible values = INACTIVE, ACTIVE, UNKNOWN

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
health	<String>	Read-only	Node Health state. Possible values = UNKNOWN, INIT, DOWN, UP, Some enabled and HAMON interfaces of the node are down, All interfaces of the node are down or disabled, SSL card(s) of the node have failed, Route Monitor(s) of the node have failed, Service state is being synchronized with the cluster, The backplane interface is either not set or it is down or is disabled, The CLAG member(s) of the node are down, Persistence sessions are being synchronized with the cluster, The Syn Cookie is being synchronized with the cluster, Unknown Health, AAA keys are being sychronized with the cluster, Cluster health is not up due

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			to config sync is in progress
syncstate	<String>	Read-only	Enable/Disable the synchronization of cluster configurations on the node. Default value: ENABLED Possible values = ENABLED, DISABLED
isconfigurationcoordinator	<Boolean>	Read-only	This argument is used to determine whether the node is configuration coordinator (CCO).
islocalnode	<Boolean>	Read-only	This argument is used to determine whether it is local node.
nodersskeymismatch	<Boolean>	Read-only	This argument is used to determine if there is a RSS key mismatch at cluster node level.
nodelicensemismatch	<Boolean>	Read-only	This argument is used to determine if there is a License mismatch at cluster node level.
nodejumbonotsupported	<Boolean>	Read-only	This argument is used to determine if Jumbo framework

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			not supported at cluster node level.
nodelist	<Integer[]>	Read-only	Nodelist for displaying Heartbeat not seen interfaces on a cluster node.
ifaceslist	<String[]>	Read-only	Interface list corresponding to nodelist for Heartbeat not seen interfaces on a cluster node.
enabledifaces	<String>	Read-only	Enabled Interfaces on a cluster node.
disabledifaces	<String>	Read-only	Disabled Interfaces on a cluster node.
partialfailifaces	<String>	Read-only	Partial Failure Interfaces on a cluster node.
hamonifaces	<String>	Read-only	Hamon Interfaces on a cluster node.
name	<String>	Read-only	Name of the state specific nodegroup. Minimum length = 1
cfgflags	<Integer>	Read-only	Flag indicates whether the node is bound to cluster nodegroup.
routemonitor	<String>	Read-only	The IP address (IPv4 or IPv6).
netmask	<String>	Read-only	The netmask.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- UPDATE
- UNSET
- DELETE
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/clusternode **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"clusternode":{

<b>"nodeid":<Integer_value>,

</b><b>"ipaddress":<String_value>,

</b>"state":<String_value>,

"backplane":<String_value>,

"priority":<Integer_value>,

"nodegroup":<String_value>,

"delay":<Integer_value>,

"tunnelmode":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/clusternode **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"clusternode":{

<b>"nodeid":<Integer_value>,

</b>"state":<String_value>,

"backplane":<String_value>,

"priority":<Integer_value>,

"delay":<Integer_value>,

"tunnelmode":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/clusternode? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"clusternode":{

<b>"nodeid":<Integer_value>,

</b>"state":true,

"backplane":true,

"priority":true,

"delay":true,

"tunnelmode":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/clusternode/ nodeid_value<Integer> **Query-parameters: args=clearnodegroupconfig: <String_value> ,force: <Boolean_value>**
get (all)
URL: http:// <netscaler-ip-address> /nitro/v1/config/clusternode **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/clusternode? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/clusternode? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of clusternode resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/clusternode? **view=summary**

Use this query-parameter to get the summary output of clusternode resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/clusternode? **pagesize=#no;pageno=#no**

Use this query-parameter to get the clusternode resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "clusternode": [ {

"nodeid":<Integer_value>,

"ipaddress":<String_value>,

"clusterhealth":<String_value>,

"effectivestate":<String_value>,

"operationalsyncstate":<String_value>,

"syncfailurereason":<String_value>,

"masterstate":<String_value>,

"health":<String_value>,

"state":<String_value>,
```

```
"backplane":<String_value>,

"syncstate":<String_value>,

"priority":<Integer_value>,

"isconfigurationcoordinator":<Boolean_value>,

"islocalnode":<Boolean_value>,

"nodersskeymismatch":<Boolean_value>,

"nodelicensemismatch":<Boolean_value>,

"nodejumbonotsupported":<Boolean_value>,

"nodelist":<Integer[]_value>,

"ifaceslist":<String[]_value>,

"enabledifaces":<String_value>,

"disabledifaces":<String_value>,

"partialfailifaces":<String_value>,

"hamonifaces":<String_value>,

"nodegroup":<String_value>,

"name":<String_value>,

"cfgflags":<Integer_value>,

"routemonitor":<String_value>,

"netmask":<String_value>,

"delay":<Integer_value>,

"tunnelmode":<String_value>,

"_nextgenapiresource":<String_value>
```

```
}]}
```

get
URL: http:// <netscaler-ip-address> /nitro/v1/config/clusternode/ nodeid_value<Integer> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/clusternode/ nodeid_value<Integer> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/clusternode/ nodeid_value<Integer> ? **view=summary**

Use this query-parameter to get the summary output of clusternode resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "clusternode": [ {

"nodeid":<Integer_value>,

"ipaddress":<String_value>,
```

```
"clusterhealth":<String_value>,

"effectivestate":<String_value>,

"operationalsyncstate":<String_value>,

"syncfailurereason":<String_value>,

"masterstate":<String_value>,

"health":<String_value>,

"state":<String_value>,

"backplane":<String_value>,

"syncstate":<String_value>,

"priority":<Integer_value>,

"isconfigurationcoordinator":<Boolean_value>,

"islocalnode":<Boolean_value>,

"nodersskeymismatch":<Boolean_value>,

"nodelicensemismatch":<Boolean_value>,

"nodejumbonotsupported":<Boolean_value>,

"nodelist":<Integer[]_value>,

"ifaceslist":<String[]_value>,

"enabledifaces":<String_value>,

"disabledifaces":<String_value>,

"partialfailifaces":<String_value>,

"hamonifaces":<String_value>,

"nodegroup":<String_value>,
```

```
"name":<String_value>,

"cfgflags":<Integer_value>,

"routemonitor":<String_value>,

"netmask":<String_value>,

"delay":<Integer_value>,

"tunnelmode":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

count

URL: http:// <netscaler-ip-address> /nitro/v1/config/clusternode? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "clusternode": [ { "__count": "#no"} ] }
```

clusternode_binding

Binding object which returns the resources bound to clusternode.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
nodeid	<Integer>	Read-write	ID of the cluster node for which to display information. If an ID is not provided, information about all nodes is shown. Default value: 255 Minimum value = 0 Maximum value = 31
clusternode_routemonitor_binding	<clusternode_routemonitor_binding[]>	Read-only	routemonitor that can be bound to clusternode.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.
- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of

creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/clusternode_binding/ nodeid_value<Integer>
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "clusternode_binding": [ {

"nodeid":<Integer_value>,

"clusternode_routemonitor_binding":<clusternode_routemonitor_binding[]_val
ue>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/clusternode_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/clusternode_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "clusternode_binding": [ {

"nodeid":<Integer_value>,

"clusternode_routemonitor_binding":<clusternode_routemonitor_binding[]_value>

}]}
```

clusternode_routemonitor_binding

Binding object showing the routemonitor that can be bound to clusternode.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
netmask	<String>	Read-write	The netmask.
nodeid	<Integer>	Read-write	A number that uniquely identifies the cluster node. . Minimum value = 0 Maximum value = 31
routemonitor	<String>	Read-write	The IP address (IPv4 or IPv6).
routemonstate	<Integer>	Read-only	Current routemonstate.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT
- ADD
- DELETE

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/clusternode_routemonitor_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"clusternode_routemonitor_binding":{

<b>"nodeid":<Integer_value>,

</b><b>"routemonitor":<String_value>,

</b>"netmask":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/clusternode_routemonitor_binding/ nodeid_value<Integer> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ clusternode_routemonitor_binding/ nodeid_value<Integer> ? **args= routemonitor:<String_value>, netmask: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/clusternode_routemonitor_binding/ nodeid_value<Integer> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ clusternode_routemonitor_binding/ nodeid_value<Integer> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of clusternode_routemonitor_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/clusternode_routemonitor_binding/ nodeid_value<Integer> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the clusternode_routemonitor_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "clusternode_routemonitor_binding": [ {

"netmask":<String_value>,

"nodeid":<Integer_value>,

"routemonitor":<String_value>,

"routemonstate":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/clusternode_routemonitor_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/clusternode_routemonitor_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "clusternode_routemonitor_binding": [ {

"netmask":<String_value>,

"nodeid":<Integer_value>,

"routemonitor":<String_value>,

"routemonstate":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/clusternode_routemonitor_binding/ nodeid_value<Integer> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"clusternode_routemonitor_binding": [ { "__count": "#no"} ] }
```

clusternodegroup

Configuration for Node group object type resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the nodegroup. The name uniquely identifies the nodegroup on the cluster. Minimum length = 1
strict	<String>	Read-write	Specifies whether cluster nodes, that are not part of the nodegroup, will be used as backup for the nodegroup. * Enabled - When one of the nodes goes down, no other cluster node is picked up to replace it. When the node comes up, it will continue being part of the nodegroup. * Disabled - When one of the nodes goes down, a non-nodegroup cluster

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			node is picked up and acts as part of the nodegroup. When the original node of the nodegroup comes up, the backup node will be replaced. Default value: NO Possible values = YES, NO
sticky	<String>	Read-write	Only one node can be bound to nodegroup with this option enabled. It specifies whether to prempt the traffic for the entities bound to nodegroup when owner node goes down and rejoins the cluster. * Enabled - When owner node goes down, backup node will become the owner node and takes the traffic for the entities bound to the nodegroup. When bound node rejoins the cluster, traffic for the entities bound to nodegroup

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			will not be steered back to this bound node. Current owner will have the ownership till it goes down. * Disabled - When one of the nodes goes down, a non-nodegroup cluster node is picked up and acts as part of the nodegroup. When the original node of the nodegroup comes up, the backup node will be replaced. Default value: NO Possible values = YES, NO
state	<String>	Read-write	State of the nodegroup. All the nodes binding to this nodegroup must have the same state. ACTIVE/SPARE/ PASSIVE. Possible values = ACTIVE, SPARE, PASSIVE

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
priority	<Integer>	Read-write	Priority of Nodegroup. This priority is used for all the nodes bound to the nodegroup for Nodegroup selection. Minimum value = 0 Maximum value = 31
currentnodemask	<Integer>	Read-only	Bitmap of current nodes in this nodegroup.
backupnodemask	<Integer>	Read-only	Bitmap of backup nodes in this nodegroup.
boundedentitiescntfrompe	<Integer>	Read-only	Count of bounded entities to this nodegroup accoding to PE.
activelist	<Integer[]>	Read-only	Active node list of this nodegroup.
backuplist	<Integer[]>	Read-only	Backup node list of this nodegroup.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- GET (ALL)
- GET

- COUNT
- UPDATE
- UNSET
- DELETE

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/clusternodegroup **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"clusternodegroup":{

<b>"name":<String_value>,

</b>"strict":<String_value>,

"sticky":<String_value>,

"state":<String_value>,

"priority":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/clusternodegroup **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"clusternodegroup":{

<b>"name":<String_value>,

</b>"strict":<String_value>,

"state":<String_value>,

"priority":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/clusternodegroup? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"clusternodegroup":{

<b>"name":<String_value>,

</b>"strict":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/clusternodegroup/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/clusternodegroup **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/clusternodegroup? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/clusternodegroup? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of clusternodegroup resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/clusternodegroup? **view=summary**

Use this query-parameter to get the summary output of clusternodegroup resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/clusternodegroup? **pagesize=#no;pageno=#no**

Use this query-parameter to get the clusternodegroup resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "clusternodegroup": [ {

"name":<String_value>,

"strict":<String_value>,

"sticky":<String_value>,

"currentnodemask":<Integer_value>,

"backupnodemask":<Integer_value>,

"boundedentitiescntfrompe":<Integer_value>,

"activelist":<Integer[]_value>,

"backuplist":<Integer[]_value>,

"state":<String_value>,

"priority":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/clusternodegroup/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/clusternodegroup/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/clusternodegroup/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of clusternodegroup resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "clusternodegroup": [ {

"name":<String_value>,

"strict":<String_value>,

"sticky":<String_value>,

"currentnodemask":<Integer_value>,

"backupnodemask":<Integer_value>,

"boundedentitiescntfrompe":<Integer_value>,

"activelist":<Integer[]_value>,

"backuplist":<Integer[]_value>,

"state":<String_value>,

"priority":<Integer_value>,

"_nextgenapiresource":<String_value>
```

```
}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/clusternodegroup? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "clusternodegroup": [ { "__count": "#no"} ] }
```

clusternodegroup_authenticationvserver_binding

Binding object showing the authenticationvserver that can be bound to clusternodegroup.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
vserver	<String>	Read-write	vserver that need to be bound to this nodegroup.
name	<String>	Read-write	Name of the nodegroup. The

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			name uniquely identifies the nodegroup on the cluster. Minimum length = 1
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT
- ADD
- DELETE

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/clusternodegroup_authenticationvserver_binding
HTTP Method: PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"clusternodegroup_authenticationvserver_binding":{

<b>"name":<String_value>,

</b>"vserver":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/ clusternodegroup_authenticationvserver_binding **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/clusternodegroup_authenticationvserver_binding? **args= name:<String_value>, vserver: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/clusternodegroup_authenticationvserver_binding **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/clusternodegroup_authenticationvserver_binding? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of clusternodegroup_authenticationvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/clusternodegroup_authenticationvserver_binding? **pagesize=#no;pageno=#no**

Use this query-parameter to get the clusternodegroup_authenticationvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "clusternodegroup_authenticationvserver_binding": [ {

"vserver":<String_value>,
```

```
"name":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/ clusternodegroup_authenticationvserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ clusternodegroup_authenticationvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "clusternodegroup_authenticationvserver_binding": [ {

"vserver":<String_value>,

"name":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/ clusternodegroup_authenticationvserver_binding? **args=;count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "clusternodegroup_authenticationvserver_binding": [ { "__count":
"#no"} ] }
```

clusternodegroup_binding

Binding object which returns the resources bound to clusternodegroup.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the nodegroup to be displayed. If a name is not provided, information about all nodegroups is displayed. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
clusternodegroup_csvserver_binding	<clusternodegroup_csvserver_binding[]>	Read-only	csvserver that can be bound to clusternodegroup.
clusternodegroup_vpnvserver_binding	<clusternodegroup_vpnvserver_binding[]>	Read-only	vpnvserver that can be bound to clusternodegroup.
clusternodegroup_streamidentifier_binding	<clusternodegroup_streamidentifier_binding[]>	Read-only	streamidentifier that can be bound to clusternodegroup.
clusternodegroup_nslimitidentifier_binding	<clusternodegroup_nslimitidentifier_binding[]>	Read-only	nslimitidentifier that can be bound to clusternodegroup.
clusternodegroup_gslbvserver_binding	<clusternodegroup_gslbvserver_binding[]>	Read-only	gslbvserver that can be bound to clusternodegroup.
clusternodegroup_clusternode_binding	<clusternodegroup_clusternode_binding[]>	Read-only	clusternode that can be bound to clusternodegroup.
clusternodegroup_gslbsite_binding	<clusternodegroup_gslbsite_binding[]>	Read-only	gslbsite that can be bound to clusternodegroup.
clusternodegroup_authenticationvserver_binding	<clusternodegroup_authenticationvserver_binding[]>	Read-only	authenticationvserver that can be bound to clusternodegroup.
clusternodegroup_crvserver_binding	<clusternodegroup_crvserver_binding[]>	Read-only	crvserver that can be bound to clusternodegroup.
clusternodegroup_lbvserver_binding	<clusternodegroup_lbvserver_binding[]>	Read-only	lbvserver that can be bound to clusternodegroup.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
clusternodegroup_service_binding	<clusternodegroup_service_binding[]>	Read-only	service that can be bound to clusternodegroup.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/clusternodegroup_binding/ name_value<String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "clusternodegroup_binding": [ {

"name":<String_value>,

"clusternodegroup_clusternode_binding":<clusternodegroup_clusternode_bindi
ng[]_value>,

"clusternodegroup_gslbsite_binding":<clusternodegroup_gslbsite_binding[]_v
alue>,

"clusternodegroup_authenticationvserver_binding":<clusternodegroup_authent
icationvserver_binding[]_value>,

"clusternodegroup_vpnvserver_binding":<clusternodegroup_vpnvserver_binding
[]_value>,

"clusternodegroup_lbvserver_binding":<clusternodegroup_lbvserver_binding[]
_value>,

"clusternodegroup_streamidentifier_binding":<clusternodegroup_streamidenti
fier_binding[]_value>,

"clusternodegroup_crvserver_binding":<clusternodegroup_crvserver_binding[]
```

```
_value>,

"clusternodegroup_service_binding":<clusternodegroup_service_binding[]_val
ue>,

"clusternodegroup_nslimitidentifier_binding":<clusternodegroup_nslimitiden
tifier_binding[]_value>,

"clusternodegroup_csvserver_binding":<clusternodegroup_csvserver_binding[]
_value>,

"clusternodegroup_gslbvserver_binding":<clusternodegroup_gslbvserver_bindi
ng[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/clusternodegroup_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/clusternodegroup_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "clusternodegroup_binding": [ {

"name":<String_value>,

"clusternodegroup_clusternode_binding":<clusternodegroup_clusternode_binding[]_value>,

"clusternodegroup_gslbsite_binding":<clusternodegroup_gslbsite_binding[]_value>,

"clusternodegroup_authenticationvserver_binding":<clusternodegroup_authenticationvserver_binding[]_value>,

"clusternodegroup_vpnvserver_binding":<clusternodegroup_vpnvserver_binding[]_value>,

"clusternodegroup_lbvserver_binding":<clusternodegroup_lbvserver_binding[]_value>,

"clusternodegroup_streamidentifier_binding":<clusternodegroup_streamidentifier_binding[]_value>,

"clusternodegroup_crvserver_binding":<clusternodegroup_crvserver_binding[]_value>,

"clusternodegroup_service_binding":<clusternodegroup_service_binding[]_value>,

"clusternodegroup_nslimitidentifier_binding":<clusternodegroup_nslimitidentifier_binding[]_value>,

"clusternodegroup_csvserver_binding":<clusternodegroup_csvserver_binding[]_value>,

"clusternodegroup_gslbvserver_binding":<clusternodegroup_gslbvserver_binding[]_value>

}]}
```

clusternodegroup_clusternode_binding

Binding object showing the clusternode that can be bound to clusternodegroup.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the nodegroup. The name uniquely identifies the nodegroup on the cluster. Minimum length = 1
node	<Integer>	Read-write	Nodes in the nodegroup. Minimum value = 0 Maximum value = 31
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT
- ADD
- DELETE

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/clusternodegroup_clusternode_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"clusternodegroup_clusternode_binding":{

<b>"name":<String_value>,

</b>"node":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/clusternodegroup_clusternode_binding **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/clusternodegroup_clusternode_binding? **args= name:<String_value>, node: <Integer_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/clusternodegroup_clusternode_binding **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/clusternodegroup_clusternode_binding? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of clusternodegroup_clusternode_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/clusternodegroup_clusternode_binding? **pagesize=#no;pageno=#no**

Use this query-parameter to get the clusternodegroup_clusternode_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "clusternodegroup_clusternode_binding": [ {

"name":<String_value>,

"node":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/clusternodegroup_clusternode_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/clusternodegroup_clusternode_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "clusternodegroup_clusternode_binding": [ {

"name":<String_value>,

"node":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/clusternodegroup_clusternode_binding?**args=;count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "clusternodegroup_clusternode_binding": [ { "__count": "#no"} ] }
```

clusternodegroup_crvserver_binding

Binding object showing the crvserver that can be bound to clusternodegroup.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
vserver	<String>	Read-write	vserver that need to be bound to this nodegroup.
name	<String>	Read-write	Name of the nodegroup. The name uniquely identifies the nodegroup on the cluster. Minimum length = 1
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT
- ADD
- DELETE

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/clusternodegroup_crvserver_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"clusternodegroup_crvserver_binding":{

<b>"name":<String_value>,

</b>"vserver":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/clusternodegroup_crvserver_binding **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/clusternodegroup_crvserver_binding? **args= name:<String_value>, vserver: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/clusternodegroup_crvserver_binding **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/clusternodegroup_crvserver_binding? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of clusternodegroup_crvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/clusternodegroup_crvserver_binding? **pagesize=#no;pageno=#no**

Use this query-parameter to get the clusternodegroup_crvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "clusternodegroup_crvserver_binding": [ {

"vserver":<String_value>,

"name":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/clusternodegroup_crvserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/clusternodegroup_crvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "clusternodegroup_crvserver_binding": [ {

"vserver":<String_value>,

"name":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/clusternodegroup_crvserver_binding?**args=;count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "clusternodegroup_crvserver_binding": [ { "__count": "#no"} ] }
```

clusternodegroup_csvserver_binding

Binding object showing the csvserver that can be bound to clusternodegroup.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
vserver	<String>	Read-write	vserver that need to be bound to this nodegroup.
name	<String>	Read-write	Name of the nodegroup. The name uniquely identifies the nodegroup on the cluster. Minimum length = 1
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT
- ADD
- DELETE

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/clusternodegroup_csvserver_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"clusternodegroup_csvserver_binding":{

<b>"name":<String_value>,

</b>"vserver":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/clusternodegroup_csvserver_binding **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/clusternodegroup_csvserver_binding? **args= name:<String_value>, vserver: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/clusternodegroup_csvserver_binding **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/clusternodegroup_csvserver_binding? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of clusternodegroup_csvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/clusternodegroup_csvserver_binding? **pagesize=#no;pageno=#no**

Use this query-parameter to get the clusternodegroup_csvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "clusternodegroup_csvserver_binding": [ {

"vserver":<String_value>,

"name":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/clusternodegroup_csvserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/clusternodegroup_csvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "clusternodegroup_csvserver_binding": [ {

"vserver":<String_value>,

"name":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/clusternodegroup_csvserver_binding?**args=;count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "clusternodegroup_csvserver_binding": [ { "__count": "#no"} ] }
```

clusternodegroup_gslbsite_binding

Binding object showing the gslbsite that can be bound to clusternodegroup.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the nodegroup. The name uniquely identifies the nodegroup on the cluster. Minimum length = 1
gslbsite	<String>	Read-write	vserver that need to be bound to this nodegroup.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT
- ADD
- DELETE

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/clusternodegroup_gslbsite_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"clusternodegroup_gslbsite_binding":{

<b>"name":<String_value>,

</b>"gslbsite":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/clusternodegroup_gslbsite_binding **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/clusternodegroup_gslbsite_binding? **args= name:<String_value>, gslbsite: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/clusternodegroup_gslbsite_binding **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/clusternodegroup_gslbsite_binding? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of clusternodegroup_gslbsite_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/clusternodegroup_gslbsite_binding? **pagesize=#no;pageno=#no**

Use this query-parameter to get the clusternodegroup_gslbsite_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "clusternodegroup_gslbsite_binding": [ {

"name":<String_value>,

"gslbsite":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/clusternodegroup_gslbsite_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/clusternodegroup_gslbsite_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "clusternodegroup_gslbsite_binding": [ {

"name":<String_value>,

"gslbsite":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/clusternodegroup_gslbsite_binding?**args=;count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "clusternodegroup_gslbsite_binding": [ { "__count": "#no"} ] }
```

clusternodegroup_gslbvserver_binding

Binding object showing the gslbvserver that can be bound to clusternodegroup.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the nodegroup. The name uniquely identifies the nodegroup on the cluster. Minimum length = 1
vserver	<String>	Read-write	vserver that need to be bound to this nodegroup.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT
- ADD
- DELETE

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/clusternodegroup_gslbvserver_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"clusternodegroup_gslbvserver_binding":{

<b>"name":<String_value>,

</b>"vserver":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/clusternodegroup_gslbvserver_binding **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/clusternodegroup_gslbvserver_binding? **args= name:<String_value>, vserver: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/clusternodegroup_gslbvserver_binding **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/clusternodegroup_gslbvserver_binding? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of clusternodegroup_gslbvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/clusternodegroup_gslbvserver_binding? **pagesize=#no;pageno=#no**

Use this query-parameter to get the clusternodegroup_gslbvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "clusternodegroup_gslbvserver_binding": [ {

"name":<String_value>,

"vserver":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/clusternodegroup_gslbvserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/clusternodegroup_gslbvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "clusternodegroup_gslbvserver_binding": [ {

"name":<String_value>,

"vserver":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/clusternodegroup_gslbvserver_binding?**args=;count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "clusternodegroup_gslbvserver_binding": [ { "__count": "#no"} ] }
```

clusternodegroup_lbvserver_binding

Binding object showing the lbvserver that can be bound to clusternodegroup.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
vserver	<String>	Read-write	vserver that need to be bound to this nodegroup.
name	<String>	Read-write	Name of the nodegroup. The name uniquely identifies the nodegroup on the cluster. Minimum length = 1
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT
- ADD
- DELETE

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/clusternodegroup_lbvserver_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"clusternodegroup_lbvserver_binding":{

<b>"name":<String_value>,

</b>"vserver":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/clusternodegroup_lbvserver_binding **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/clusternodegroup_lbvserver_binding? **args= name:<String_value>, vserver: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/clusternodegroup_lbvserver_binding **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/clusternodegroup_lbvserver_binding? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of clusternodegroup_lbvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/clusternodegroup_lbvserver_binding? **pagesize=#no;pageno=#no**

Use this query-parameter to get the clusternodegroup_lbvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "clusternodegroup_lbvserver_binding": [ {

"vserver":<String_value>,

"name":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/clusternodegroup_lbvserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/clusternodegroup_lbvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "clusternodegroup_lbvserver_binding": [ {

"vserver":<String_value>,

"name":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/clusternodegroup_lbvserver_binding?**args=;count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "clusternodegroup_lbvserver_binding": [ { "__count": "#no"} ] }
```

clusternodegroup_nslimitidentifier_binding

Binding object showing the nslimitidentifier that can be bound to clusternodegroup.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the nodegroup to which you want to bind a cluster node or an entity. Minimum length = 1
identifiername	<String>	Read-write	stream identifier and rate limit identifier that need to be bound to this nodegroup.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT
- ADD
- DELETE

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of

creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/clusternodegroup_nslimitidentifier_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"clusternodegroup_nslimitidentifier_binding":{

<b>"name":<String_value>,

</b>"identifiername":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/clusternodegroup_nslimitidentifier_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ clusternodegroup_nslimitidentifier_binding/ name_value<String> ? **args=identifiername: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/clusternodegroup_nslimitidentifier_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ clusternodegroup_nslimitidentifier_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of clusternodegroup_nslimitidentifier_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ clusternodegroup_nslimitidentifier_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the clusternodegroup_nslimitidentifier_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "clusternodegroup_nslimitidentifier_binding": [ {

"name":<String_value>,

"identifiername":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/clusternodegroup_nslimitidentifier_binding
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/clusternodegroup_nslimitidentifier_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "clusternodegroup_nslimitidentifier_binding": [ {

"name":<String_value>,

"identifiername":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/clusternodegroup_nslimitidentifier_binding/name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"clusternodegroup_nslimitidentifier_binding": [ { "__count": "#no"} ] }
```

clusternodegroup_service_binding

Binding object showing the service that can be bound to clusternodegroup.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
service	<String>	Read-write	name of the service bound to this nodegroup.
name	<String>	Read-write	Name of the nodegroup. The name uniquely identifies the nodegroup on the cluster. Minimum length = 1
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT
- ADD
- DELETE

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/clusternodegroup_service_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"clusternodegroup_service_binding":{

<b>"name":<String_value>,

</b>"service":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/clusternodegroup_service_binding **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/clusternodegroup_service_binding? **args= name:<String_value>, service: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/clusternodegroup_service_binding **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/clusternodegroup_service_binding? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of clusternodegroup_service_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/clusternodegroup_service_binding? **pagesize=#no;pageno=#no**

Use this query-parameter to get the clusternodegroup_service_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "clusternodegroup_service_binding": [ {

"service":<String_value>,

"name":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/clusternodegroup_service_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/clusternodegroup_service_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "clusternodegroup_service_binding": [ {

"service":<String_value>,

"name":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/clusternodegroup_service_binding?**args=;count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "clusternodegroup_service_binding": [ { "__count": "#no"} ] }
```

clusternodegroup_streamidentifier_binding

Binding object showing the streamidentifier that can be bound to clusternodegroup.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the nodegroup to which you want to bind a cluster node or an entity. Minimum length = 1
identifiername	<String>	Read-write	stream identifier and rate limit identifier that need to be bound to this nodegroup.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT
- ADD
- DELETE

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of

creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/clusternodegroup_streamidentifier_binding
HTTP Method: PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"clusternodegroup_streamidentifier_binding":{

<b>"name":<String_value>,

</b>"identifiername":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/clusternodegroup_streamidentifier_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ clusternodegroup_streamidentifier_binding/ name_value<String> ? **args=identifiername: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/clusternodegroup_streamidentifier_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ clusternodegroup_streamidentifier_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of clusternodegroup_streamidentifier_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ clusternodegroup_streamidentifier_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the clusternodegroup_streamidentifier_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "clusternodegroup_streamidentifier_binding": [ {

"name":<String_value>,

"identifiername":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/clusternodegroup_streamidentifier_binding
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/clusternodegroup_streamidentifier_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "clusternodegroup_streamidentifier_binding": [ {

"name":<String_value>,

"identifiername":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/clusternodegroup_streamidentifier_binding/name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"clusternodegroup_streamidentifier_binding": [ { "__count": "#no"} ] }
```

clusternodegroup_vpnvserver_binding

Binding object showing the vpnvserver that can be bound to clusternodegroup.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
vserver	<String>	Read-write	vserver that need to be bound to this nodegroup.
name	<String>	Read-write	Name of the nodegroup. The name uniquely identifies the nodegroup on the cluster. Minimum length = 1
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT
- ADD
- DELETE

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/clusternodegroup_vpnvserver_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"clusternodegroup_vpnvserver_binding":{

<b>"name":<String_value>,

</b>"vserver":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/clusternodegroup_vpnvserver_binding **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/clusternodegroup_vpnvserver_binding? **args= name:<String_value>, vserver: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/clusternodegroup_vpnvserver_binding **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/clusternodegroup_vpnvserver_binding? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of clusternodegroup_vpnvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/clusternodegroup_vpnvserver_binding? **pagesize=#no;pageno=#no**

Use this query-parameter to get the clusternodegroup_vpnvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "clusternodegroup_vpnvserver_binding": [ {

"vserver":<String_value>,

"name":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/clusternodegroup_vpnvserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/clusternodegroup_vpnvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "clusternodegroup_vpnvserver_binding": [ {

"vserver":<String_value>,

"name":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/clusternodegroup_vpnvserver_binding?**args=;count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "clusternodegroup_vpnvserver_binding": [ { "__count": "#no"} ] }
```

clusterpropstatus

Configuration for 0 resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
nodeid	<Integer>	Read-write	Unique number that identifies the cluster node. Minimum value = 0 Maximum value = 31
numpropcmdfailed	<Integer>	Read-only	Number of propogated comands failed on this node. Minimum value = 0 Maximum value = 20
cmdstrs	<String>	Read-only	.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET (ALL)
- COUNT
- CLEAR

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

CLEAR

URL: http:// <netscaler-ip-address> /nitro/v1/config/clusterpropstatus? **action=clear HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"clusterpropstatus":{

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/clusterpropstatus **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/clusterpropstatus? **args=nodeid: <Integer_value>**

Use this query-parameter to get clusterpropstatus resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/config/clusterpropstatus? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/clusterpropstatus? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of clusterpropstatus resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/clusterpropstatus? **view=summary**

Use this query-parameter to get the summary output of clusterpropstatus resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/clusterpropstatus? **pagesize=#no;pageno=#no**

Use this query-parameter to get the clusterpropstatus resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "clusterpropstatus": [ {

nodeid:<Integer_value>"numpropcmdfailed":<Integer_value>,

"cmdstrs":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/clusterpropstatus? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "clusterpropstatus": [ { "__count": "#no"} ] }
```

clustersync

Configuration for sync resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION

Operations

(click to see Properties)

- FORCE

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

FORCE

URL: http:// <netscaler-ip-address> /nitro/v1/config/clustersync? **action=Force**

HTTP Method: POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"clustersync":{

}}
```

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

clustersyncfailures

Configuration for Cluster sync failures resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
_nextgenapiresource	<String>	Read-write	.

Operations

(click to see Properties)

- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/clustersyncfailures

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "clustersyncfailures": [ {

"_nextgenapiresource":<String_value>

}]}
```

cmp

Compression

Compression configuration. The system's feature for compressing HTTP responses to compression-aware browsers.

NAME	DESCRIPTION
cmpaction	Configuration for compression action
cmpglobal_binding	Binding object showing the resources that can be bound to cmpglobal
cmpglobal_cmppolicy_binding	Binding object showing the cmppolicy that can be bound to cmpglobal
cmpparameter	Configuration for CMP parameter
cmppolicy	Configuration for compression policy
cmppolicy_binding	Binding object showing the resources that can be bound to cmppolicy
cmppolicy_cmpglobal_binding	Binding object showing the cmpglobal that can be bound to cmppolicy

NAME	DESCRIPTION
cmppolicy_cmppolicylabel_binding	Binding object showing the cmppolicylabel that can be bound to cmppolicy
cmppolicy_crvserver_binding	Binding object showing the crvserver that can be bound to cmppolicy
cmppolicy_csvserver_binding	Binding object showing the csvserver that can be bound to cmppolicy
cmppolicy_lbvserver_binding	Binding object showing the lbvserver that can be bound to cmppolicy
cmppolicylabel	Configuration for compression policy label
cmppolicylabel_binding	Binding object showing the resources that can be bound to cmppolicylabel
cmppolicylabel_cmppolicy_binding	Binding object showing the cmppolicy that can be bound to cmppolicylabel
cmppolicylabel_policybinding_binding	Binding object showing the policybinding that can be bound to cmppolicylabel

cmpaction

Configuration for compression action resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the compression action. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Can be changed after the action is added. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my cmp action" or 'my cmp action'). Minimum length = 1
cmptype	<String>	Read-write	Type of compression performed by this action. Available settings function as follows:

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			* COMPRESS - Apply GZIP or DEFLATE compression to the response, depending on the request header. Prefer GZIP. * GZIP - Apply GZIP compression. * DEFLATE - Apply DEFLATE compression. * NOCOMPRESS - Do not compress the response if the request matches a policy that uses this action. Possible values = compress, gzip, deflate, nocompress
addvaryheader	<String>	Read-write	Control insertion of the Vary header in HTTP responses compressed by Citrix ADC. Intermediate caches store different versions of the response for different values of the headers present in the Vary response header.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: GLOBAL Possible values = GLOBAL, DISABLED, ENABLED
varyheadervalue	<String>	Read-write	The value of the HTTP Vary header for compressed responses. Minimum length = 1
deltatype	<String>	Read-write	The type of delta action (if delta type compression action is defined). Default value: PERURL Possible values = PERURL, PERPOLICY
newname	<String>	Read-write	New name for the compression action. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Choose a name that can be correlated with the function that the action performs. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my cmp action" or 'my cmp action'). Minimum length = 1
builtin	<String[]>	Read-only	Flag to determine whether compression is default or not. Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL
feature	<String>	Read-only	The feature to be checked while applying this config.
isdefault	<Boolean>	Read-only	A value of true is returned if it is a default policy.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET (ALL)
- GET
- COUNT
- UPDATE
- UNSET
- RENAME

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/cmpaction **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"cmpaction":{

<b>"name":<String_value>,

</b><b>"cmptype":<String_value>,

</b>"addvaryheader":<String_value>,

"varyheadervalue":<String_value>,

"deltatype":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/cmpaction/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/cmpaction **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"cmpaction":{

<b>"name":<String_value>,

</b>"cmptype":<String_value>,

"addvaryheader":<String_value>,

"varyheadervalue":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/cmpaction? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"cmpaction":{

<b>"name":<String_value>,

</b>"addvaryheader":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

RENAME

URL: http:// <netscaler-ip-address> /nitro/v1/config/cmpaction? **action=rename HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"cmpaction":{

<b>"name":<String_value>,

</b><b>"newname":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/cmpaction **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/cmpaction? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/cmpaction? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of cmpaction resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/cmpaction? **view=summary**

Use this query-parameter to get the summary output of cmpaction resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/cmpaction? **pagesize=#no;pageno=#no**

Use this query-parameter to get the cmpaction resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "cmpaction": [ {

"name":<String_value>,
```

```
"cmptype":<String_value>,

"deltatype":<String_value>,

"addvaryheader":<String_value>,

"varyheadervalue":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"isdefault":<Boolean_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/cmpaction/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/cmpaction/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/cmpaction/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of cmpaction resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "cmpaction": [ {

"name":<String_value>,

"cmptype":<String_value>,

"deltatype":<String_value>,

"addvaryheader":<String_value>,

"varyheadervalue":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"isdefault":<Boolean_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/cmpaction? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "cmpaction": [ { "__count": "#no"} ] }
```

cmpglobal_binding

Binding object which returns the resources bound to cmpglobal.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
cmpglobal_cmppolicy_binding	<cmpglobal_cmppolicy_binding[]>	Read-write	cmppolicy that can be bound to cmpglobal.

Operations

(click to see Properties)

- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/cmpglobal_binding

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "cmpglobal_binding": [ {

"cmpglobal_cmppolicy_binding":<cmpglobal_cmppolicy_binding[]_value>
```

```
}]}
```

cmpglobal_cmppolicy_binding

Binding object showing the cmppolicy that can be bound to cmpglobal.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
gotopriorityexpression	<String>	Read-write	Expression or other value specifying the priority of the next policy, within the policy label, to evaluate if the current policy evaluates to TRUE. Specify one of the following values: * NEXT - Evaluate the policy with the next higher numbered priority. * END - Stop evaluation. * USE_INVOCATION_RESULT - Applicable if this policy invokes another policy label. If the final goto in the invoked policy label has a value of END, the evaluation stops. If the final goto is anything other than END, the current policy label performs a NEXT. * An

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			expression that evaluates to a number. If you specify an expression, it's evaluation result determines the next policy to evaluate, as follows: * If the expression evaluates to a higher numbered priority, that policy is evaluated next. * If the expression evaluates to the priority of the current policy, the policy with the next higher priority number is evaluated next. * If the expression evaluates to a priority number that is numerically higher than the highest priority number, policy evaluation ends. An UNDEF event is triggered if: * The expression is invalid. * The expression evaluates to a priority number that is numerically lower than the current policy's priority. * The expression evaluates to a priority number that is between the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			current policy's priority number (say, 30) and the highest priority number (say, 100), but does not match any configured priority number (for example, the expression evaluates to the number 85). This example assumes that the priority number increments by 10 for every successive policy, and therefore a priority number of 85 does not exist in the policy label.
invoke	<Boolean>	Read-write	Invoke policies bound to a virtual server or a policy label. After the invoked policies are evaluated, the flow returns to the policy with the next priority.
globalbindtype	<String>	Read-write	. Default value: SYSTEM_GLOBAL Possible values = SYSTEM_GLOBAL, VPN_GLOBAL, RNAT_GLOBAL, APPFW_GLOBAL, TM_GLOBAL

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
policyname	<String>	Read-write	The name of the globally bound HTTP compression policy.
type	<String>	Read-write	Bind point to which the policy is bound. Possible values = REQ_OVERRIDE, REQ_DEFAULT, RES_OVERRIDE, RES_DEFAULT, HTTPQUIC_REQ_OVERRIDE, HTTPQUIC_REQ_DEFAULT, HTTPQUIC_RES_OVERRIDE, HTTPQUIC_RES_DEFAULT
labelname	<String>	Read-write	Name of the label to invoke if the current policy rule evaluates to TRUE.
labeltype	<String>	Read-write	Type of policy label invocation. Possible values = reqvserver, resvserver, policylabel
priority	<Integer>	Read-write	Positive integer specifying the priority of the policy. The lower the number, the higher the priority. By default, polices within a label

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			are evaluated in the order of their priority numbers. In the configuration utility, you can click the Priority field and edit the priority level or drag the entry to a new position in the list. If you drag the entry to a new position, the priority level is updated automatically.
numpol	<Integer>	Read-only	The number of policies bound to the bindpoint.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/cmpglobal_cmppolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"cmpglobal_cmppolicy_binding":{

<b>"policyname":<String_value>,

</b>"priority":<Integer_value>,

"gotopriorityexpression":<String_value>,

"type":<String_value>,

"invoke":<Boolean_value>,
```

```
"labeltype":<String_value>,

"labelname":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/cmpglobal_cmppolicy_binding **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/cmpglobal_cmppolicy_binding? **args= policyname:<String_value>, type: <String_value> ,priority: <Integer_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/cmpglobal_cmppolicy_binding **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/cmpglobal_cmppolicy_binding? **args=type: <String_value>**

Use this query-parameter to get cmpglobal_cmppolicy_binding resources based on additional properties.

filter http:// <netscaler-ip-address> /nitro/v1/config/cmpglobal_cmppolicy_binding? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of cmpglobal_cmppolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/cmpglobal_cmppolicy_binding? **pagesize=#no;pageno=#no**

Use this query-parameter to get the cmpglobal_cmppolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "cmpglobal_cmppolicy_binding": [ {

"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>,

"globalbindtype":<String_value>,

"policyname":<String_value>,

"type":<String_value>,

"labelname":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"numpol":<Integer_value>
```

```
}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/cmpglobal_cmppolicy_binding? **count=yes**
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "cmpglobal_cmppolicy_binding": [ { "__count": "#no"} ] }
```

cmpparameter

Configuration for CMP parameter resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
cmplevel	<String>	Read-write	Specify a compression level. Available settings function as follows:

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			* Optimal - Corresponds to a gzip GZIP level of 5-7. * Best speed - Corresponds to a gzip level of 1. * Best compression - Corresponds to a gzip level of 9. Default value: optimal Possible values = optimal, bestspeed, bestcompression
quantumsize	<Integer>	Read-write	Minimum quantum of data to be filled before compression begins. Default value: 57344 Minimum value = 8 Maximum value = 63488
servercmp	<String>	Read-write	Allow the server to send compressed data to the Citrix ADC. With the default setting, the Citrix ADC appliance handles all compression.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: ON Possible values = ON, OFF
heurexpiry	<String>	Read-write	Heuristic basefile expiry. Default value: OFF Possible values = ON, OFF
heurexpirythres	<Integer>	Read-write	Threshold compression ratio for heuristic basefile expiry, multiplied by 100. For example, to set the threshold ratio to 1.25, specify 125. Default value: 100 Minimum value = 1 Maximum value = 1000
heurexpiryhistwt	<Integer>	Read-write	For heuristic basefile expiry, weightage to be given to historical delta compression ratio, specified as percentage. For example, to give 25% weightage to historical ratio (and therefore 75% weightage to the ratio for current delta compression

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			transaction), specify 25. Default value: 50 Minimum value = 1 Maximum value = 100
minressize	<Integer>	Read-write	Smallest response size, in bytes, to be compressed.
cmpbypasspct	<Integer>	Read-write	Citrix ADC CPU threshold after which compression is not performed. Range: 0 - 100. Default value: 100 Minimum value = 0 Maximum value = 100
cmponpush	<String>	Read-write	Citrix ADC does not wait for the quantum to be filled before starting to compress data. Upon receipt of a packet with a PUSH flag, the appliance immediately begins compression of the accumulated packets. Default value: DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ENABLED, DISABLED
policytype	<String>	Read-write	Type of the policy. The only possible value is ADVANCED. Default value: ADVANCED Possible values = ADVANCED
addvaryheader	<String>	Read-write	Control insertion of the Vary header in HTTP responses compressed by Citrix ADC. Intermediate caches store different versions of the response for different values of the headers present in the Vary response header. Default value: DISABLED Possible values = ENABLED, DISABLED
varyheadervalue	<String>	Read-write	The value of the HTTP Vary header for compressed responses. If this argument is not specified, a default value of "Accept-

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Encoding" will be used. Minimum length = 1
externalcache	<String>	Read-write	Enable insertion of Cache-Control: private response directive to indicate response message is intended for a single user and must not be cached by a shared or proxy cache. Default value: NO Possible values = YES, NO
randomgzipfilename	<String>	Read-write	Control the addition of a random filename of random length in the GZIP header to apply the Heal-the-BREACH mitigation for the BREACH attack. Default value: DISABLED Possible values = ENABLED, DISABLED
randomgzipfilename minlength	<Integer>	Read-write	Minimum length of the random filename to be added in the GZIP header to apply the Heal-the-BREACH mitigation

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			for the BREACH attack. Default value: 8 Minimum value = 8 Maximum value = 63
randomgzipfilenamemaxlength	<Integer>	Read-write	Maximum length of the random filename to be added in the GZIP header to apply the Heal-the-BREACH mitigation for the BREACH attack. Default value: 63 Minimum value = 8 Maximum value = 63
builtin	<String[]>	Read-only	Flag to determine whether compression is default or not. Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL
feature	<String>	Read-only	The feature to be checked while applying this config.
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- UPDATE
- UNSET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/cmpparameter **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"cmpparameter":{

"cmplevel":<String_value>,

"quantumsize":<Integer_value>,

"servercmp":<String_value>,

"heurexpiry":<String_value>,

"heurexpirythres":<Integer_value>,

"heurexpiryhistwt":<Integer_value>,

"minressize":<Integer_value>,

"cmpbypasspct":<Integer_value>,

"cmponpush":<String_value>,

"policytype":<String_value>,

"addvaryheader":<String_value>,

"varyheadervalue":<String_value>,

"externalcache":<String_value>,

"randomgzipfilename":<String_value>,

"randomgzipfilenameminlength":<Integer_value>,

"randomgzipfilenamemaxlength":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/cmpparameter? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"cmpparameter":{

"policytype":true,

"cmplevel":true,

"quantumsize":true,

"servercmp":true,

"heurexpiry":true,

"heurexpirythres":true,

"heurexpiryhistwt":true,

"minressize":true,

"cmpbypasspct":true,

"cmponpush":true,

"addvaryheader":true,

"varyheadervalue":true,

"externalcache":true,

"randomgzipfilename":true,

"randomgzipfilenameminlength":true,
```

```
"randomgzipfilenamemaxlength":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/cmpparameter **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "cmpparameter": [ {

"cmplevel":<String_value>,

"quantumsize":<Integer_value>,

"servercmp":<String_value>,

"heurexpiry":<String_value>,

"heurexpirythres":<Integer_value>,

"heurexpiryhistwt":<Integer_value>,
```

```
"minressize":<Integer_value>,

"cmpbypasspct":<Integer_value>,

"cmponpush":<String_value>,

"policytype":<String_value>,

"addvaryheader":<String_value>,

"varyheadervalue":<String_value>,

"externalcache":<String_value>,

"randomgzipfilename":<String_value>,

"randomgzipfilenameminlength":<Integer_value>,

"randomgzipfilenamemaxlength":<Integer_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

cmppolicy

Configuration for compression policy resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the HTTP compression policy. Must begin with an ASCII alphabetic or

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Can be changed after the policy is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my cmp policy" or 'my cmp policy'). Minimum length = 1
rule	<String>	Read-write	Expression that determines which HTTP requests or responses match the compression policy. The following requirements apply

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			only to the Citrix ADC CLI: * If the expression includes one or more spaces, enclose the entire expression in double quotation marks. * If the expression itself includes double quotation marks, escape the quotations by using the \ character. * Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks.
resaction	<String>	Read-write	The built-in or user-defined compression action to apply to the response when the policy matches a request or response. Minimum length = 1
newname	<String>	Read-write	New name for the compression policy. Must begin with an ASCII alphabetic or

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Choose a name that reflects the function that the policy performs. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my cmp policy" or 'my cmp policy'). Minimum length = 1
reqaction	<String>	Read-only	The compression action to be performed on requests.
hits	<Integer>	Read-only	Number of hits.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
txbytes	<Integer>	Read-only	Number of bytes transferred.
rxbytes	<Integer>	Read-only	Number of bytes received.
clientttlb	<Integer>	Read-only	Total client TTLB value.
clienttransactions	<Integer>	Read-only	Number of client transactions.
serverttlb	<Integer>	Read-only	Total server TTLB value.
servertransactions	<Integer>	Read-only	Number of server transactions.
description	<String>	Read-only	Description of the policy.
builtin	<String[]>	Read-only	Flag to determine if compression policy is builtin or not. Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL
feature	<String>	Read-only	The feature to be checked while applying this config.
isdefault	<Boolean>	Read-only	A value of true is returned if it is a default policy.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- GET (ALL)
- GET
- COUNT
- RENAME

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/cmppolicy **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"cmppolicy":{

<b>"name":<String_value>,

</b><b>"rule":<String_value>,

</b><b>"resaction":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/cmppolicy/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/cmppolicy **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"cmppolicy":{

<b>"name":<String_value>,

</b>"rule":<String_value>,

"resaction":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

RENAME

URL: http:// <netscaler-ip-address> /nitro/v1/config/cmppolicy? **action=rename HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"cmppolicy":{

<b>"name":<String_value>,

</b><b>"newname":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/cmppolicy **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/cmppolicy? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/cmppolicy? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of cmppolicy resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/cmppolicy? **view=summary**

Use this query-parameter to get the summary output of cmppolicy resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/cmppolicy? **pagesize=#no;pageno=#no**

Use this query-parameter to get the cmppolicy resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "cmppolicy": [ {

"name":<String_value>,

"rule":<String_value>,

"reqaction":<String_value>,

"resaction":<String_value>,

"hits":<Integer_value>,

"txbytes":<Integer_value>,

"rxbytes":<Integer_value>,

"clientttlb":<Integer_value>,

"clienttransactions":<Integer_value>,

"serverttlb":<Integer_value>,

"servertransactions":<Integer_value>,

"description":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"isdefault":<Boolean_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/cmppolicy/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/cmppolicy/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/cmppolicy/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of cmppolicy resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "cmppolicy": [ {

"name":<String_value>,

"rule":<String_value>,

"reqaction":<String_value>,

"resaction":<String_value>,

"hits":<Integer_value>,

"txbytes":<Integer_value>,

"rxbytes":<Integer_value>,
```

```
"clientttlb":<Integer_value>,

"clienttransactions":<Integer_value>,

"serverttlb":<Integer_value>,

"servertransactions":<Integer_value>,

"description":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"isdefault":<Boolean_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/cmppolicy? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "cmppolicy": [ { "__count": "#no"} ] }
```

cmppolicy_binding

Binding object which returns the resources bound to cmppolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the HTTP compression policy for which to display details. Minimum length = 1
cmppolicy_crvserver_binding	<cmppolicy_crvserver_binding[]>	Read-only	crvserver that can be bound to cmppolicy.
cmppolicy_lbvserver_binding	<cmppolicy_lbvserver_binding[]>	Read-only	lbvserver that can be bound to cmppolicy.
cmppolicy_cmppolicylabel_binding	<cmppolicy_cmppolicylabel_binding[]>	Read-only	cmppolicylabel that can be bound to cmppolicy.
cmppolicy_cmpglobal_binding	<cmppolicy_cmpglobal_binding[]>	Read-only	cmpglobal that can be bound to cmppolicy.
cmppolicy_csvserver_binding	<cmppolicy_csvserver_binding[]>	Read-only	csvserver that can be bound to cmppolicy.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/cmppolicy_binding/ name_value<String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "cmppolicy_binding": [ {

"name":<String_value>,

"cmppolicy_cmppolicylabel_binding":<cmppolicy_cmppolicylabel_binding[]_val
ue>,

"cmppolicy_lbvserver_binding":<cmppolicy_lbvserver_binding[]_value>,

"cmppolicy_csvserver_binding":<cmppolicy_csvserver_binding[]_value>,

"cmppolicy_crvserver_binding":<cmppolicy_crvserver_binding[]_value>,

"cmppolicy_cmpglobal_binding":<cmppolicy_cmpglobal_binding[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/cmppolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/cmppolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "cmppolicy_binding": [ {

"name":<String_value>,

"cmppolicy_cmppolicylabel_binding":<cmppolicy_cmppolicylabel_binding[]_value>,

"cmppolicy_lbvserver_binding":<cmppolicy_lbvserver_binding[]_value>,

"cmppolicy_csvserver_binding":<cmppolicy_csvserver_binding[]_value>,

"cmppolicy_crvserver_binding":<cmppolicy_crvserver_binding[]_value>,

"cmppolicy_cmpglobal_binding":<cmppolicy_cmpglobal_binding[]_value>

}]}
```

cmppolicy_cmpglobal_binding

Binding object showing the cmpglobal that can be bound to cmppolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
boundto	<String>	Read-write	The name of the entity to which the policy is bound.
name	<String>	Read-write	Name of the HTTP compression policy for which to display details. Minimum length = 1
activepolicy	<Integer>	Read-only	.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
gotopriorityexpression	<String>	Read-only	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
labelname	<String>	Read-only	Name of the label to invoke if the current policy rule evaluates to TRUE.
priority	<Integer>	Read-only	.
labeltype	<String>	Read-only	Type of policy label invocation. Possible values = reqvserver, resvserver, policylabel
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/cmppolicy_cmpglobal_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ cmppolicy_cmpglobal_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of cmppolicy_cmpglobal_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/cmppolicy_cmpglobal_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the cmppolicy_cmpglobal_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "cmppolicy_cmpglobal_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"activepolicy":<Integer_value>,

"gotopriorityexpression":<String_value>,

"labelname":<String_value>,

"priority":<Integer_value>,

"labeltype":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/cmppolicy_cmpglobal_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/cmppolicy_cmpglobal_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "cmppolicy_cmpglobal_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"activepolicy":<Integer_value>,

"gotopriorityexpression":<String_value>,

"labelname":<String_value>,

"priority":<Integer_value>,

"labeltype":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/cmppolicy_cmpglobal_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"cmppolicy_cmpglobal_binding": [ { "__count": "#no"} ] }
```

cmppolicy_cmppolicylabel_binding

Binding object showing the cmppolicylabel that can be bound to cmppolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
boundto	<String>	Read-write	The name of the entity to which the policy is bound.
name	<String>	Read-write	Name of the HTTP compression policy for which to display details. Minimum length = 1
labeltype	<String>	Read-only	Type of policy label invocation. Possible values = reqvserver, resvserver, policylabel
priority	<Integer>	Read-only	.
labelname	<String>	Read-only	Name of the label to invoke if the current

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			policy rule evaluates to TRUE.
gotopriorityexpression	<String>	Read-only	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
activepolicy	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/cmppolicy_cmppolicylabel_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ cmppolicy_cmppolicylabel_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of cmppolicy_cmppolicylabel_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/cmppolicy_cmppolicylabel_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the cmppolicy_cmppolicylabel_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "cmppolicy_cmppolicylabel_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"labelname":<String_value>,

"gotopriorityexpression":<String_value>,

"activepolicy":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/cmppolicy_cmppolicylabel_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/cmppolicy_cmppolicylabel_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "cmppolicy_cmppolicylabel_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"labelname":<String_value>,

"gotopriorityexpression":<String_value>,

"activepolicy":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/cmppolicy_cmppolicylabel_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"cmppolicy_cmppolicylabel_binding": [ { "__count": "#no"} ] }
```

cmppolicy_crvserver_binding

Binding object showing the crvserver that can be bound to cmppolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the HTTP compression policy for which to display details. Minimum length = 1
boundto	<String>	Read-write	The name of the entity to which the policy is bound.
priority	<Integer>	Read-only	.
activepolicy	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/cmppolicy_crvserver_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ cmppolicy_crvserver_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of cmppolicy_crvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/cmppolicy_crvserver_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the cmppolicy_crvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "cmppolicy_crvserver_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"priority":<Integer_value>,

"activepolicy":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/cmppolicy_crvserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/cmppolicy_crvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "cmppolicy_crvserver_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"priority":<Integer_value>,

"activepolicy":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/cmppolicy_crvserver_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"cmppolicy_crvserver_binding": [ { "__count": "#no"} ] }
```

cmppolicy_csvserver_binding

Binding object showing the csvserver that can be bound to cmppolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the HTTP compression policy for which to display details. Minimum length = 1
boundto	<String>	Read-write	The name of the entity to which the policy is bound.
priority	<Integer>	Read-only	.
labeltype	<String>	Read-only	Type of policy label invocation. Possible values = reqvserver, resvserver, policylabel
activepolicy	<Integer>	Read-only	.
gotopriorityexpression	<String>	Read-only	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
labelname	<String>	Read-only	Name of the label to invoke if the current policy rule evaluates to TRUE.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/cmppolicy_csvserver_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ cmppolicy_csvserver_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of cmppolicy_csvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/cmppolicy_csvserver_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the cmppolicy_csvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "cmppolicy_csvserver_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"priority":<Integer_value>,

"labeltype":<String_value>,
```

```
"activepolicy":<Integer_value>,

"gotopriorityexpression":<String_value>,

"labelname":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/cmppolicy_csvserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/cmppolicy_csvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "cmppolicy_csvserver_binding": [ {

"name":<String_value>,

"boundto":<String_value>,
```

```
"priority":<Integer_value>,

"labeltype":<String_value>,

"activepolicy":<Integer_value>,

"gotopriorityexpression":<String_value>,

"labelname":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/cmppolicy_csvserver_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"cmppolicy_csvserver_binding": [ { "__count": "#no"} ] }
```

cmppolicy_lbvserver_binding

Binding object showing the lbvserver that can be bound to cmppolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
boundto	<String>	Read-write	The name of the entity to which the policy is bound.
name	<String>	Read-write	Name of the HTTP compression policy for which to display details. Minimum length = 1
priority	<Integer>	Read-only	.
labeltype	<String>	Read-only	Type of policy label invocation. Possible values = reqvserver, resvserver, policylabel
activepolicy	<Integer>	Read-only	.
gotopriorityexpression	<String>	Read-only	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
labelname	<String>	Read-only	Name of the label to invoke if the current policy rule evaluates to TRUE.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/cmppolicy_lbvserver_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ cmppolicy_lbvserver_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of cmppolicy_lbvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/cmppolicy_lbvserver_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the cmppolicy_lbvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "cmppolicy_lbvserver_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"priority":<Integer_value>,

"labeltype":<String_value>,

"activepolicy":<Integer_value>,

"gotopriorityexpression":<String_value>,

"labelname":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/cmppolicy_lbvserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/cmppolicy_lbvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "cmppolicy_lbvserver_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"priority":<Integer_value>,

"labeltype":<String_value>,

"activepolicy":<Integer_value>,

"gotopriorityexpression":<String_value>,
```

```
"labelname":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/cmppolicy_lbvserver_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"cmppolicy_lbvserver_binding": [ { "__count": "#no"} ] }
```

cmppolicylabel

Configuration for compression policy label resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
labelname	<String>	Read-write	Name of the HTTP compression policy label. Must begin with a letter, number,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			or the underscore character (_). Additional characters allowed, after the first character, are the hyphen (-), period (.) pound sign (#), space ( ), at sign (@), equals (=), and colon (:). The name must be unique within the list of policy labels for compression policies. Can be renamed after the policy label is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my cmp policylabel" or 'my cmp policylabel'). Minimum length = 1
type	<String>	Read-write	Type of packets (request packets or response) against which to match the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			policies bound to this policy label. Possible values = REQ, RES, HTTPQUIC_REQ, HTTPQUIC_RES
newname	<String>	Read-write	New name for the compression policy label. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my cmp policylabel" or 'my cmp policylabel'). Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
numpol	<Integer>	Read-only	Number of polices bound to label.
hits	<Integer>	Read-only	Number of times policy label was invoked.
priority	<Integer>	Read-only	Specifies the priority of the policy.
gotopriorityexpression	<String>	Read-only	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
labeltype	<String>	Read-only	Type of policy label invocation. Possible values = reqvserver, resvserver, policylabel
invoke_labelname	<String>	Read-only	Name of the label to invoke if the current policy evaluates to TRUE.
flowtype	<Integer>	Read-only	Flowtype of the bound compression policy.
description	<String>	Read-only	Description of the policylabel.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET (ALL)
- GET
- COUNT
- RENAME

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/cmppolicylabel **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"cmppolicylabel":{

<b>"labelname":<String_value>,

</b><b>"type":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/cmppolicylabel/ labelname_value<String>
HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

RENAME

URL: http:// <netscaler-ip-address> /nitro/v1/config/cmppolicylabel? **action=rename HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"cmppolicylabel":{

<b>"labelname":<String_value>,

</b><b>"newname":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/cmppolicylabel **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/cmppolicylabel? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/cmppolicylabel? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of cmppolicylabel resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/cmppolicylabel? **view=summary**

Use this query-parameter to get the summary output of cmppolicylabel resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/cmppolicylabel? **pagesize=#no;pageno=#no**

Use this query-parameter to get the cmppolicylabel resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "cmppolicylabel": [ {

"labelname":<String_value>,

"type":<String_value>,

"numpol":<Integer_value>,

"hits":<Integer_value>,

"priority":<Integer_value>,

"gotopriorityexpression":<String_value>,

"labeltype":<String_value>,

"invoke_labelname":<String_value>,

"flowtype":<Integer_value>,

"description":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/cmppolicylabel/ labelname_value<String>
Query-parameters: attrs http:// <netscaler-ip-address> /nitro/v1/config/cmppolicylabel/ labelname_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/cmppolicylabel/ labelname_value<String> ? **view=summary**

Use this query-parameter to get the summary output of cmppolicylabel resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "cmppolicylabel": [ {

"labelname":<String_value>,

"type":<String_value>,

"numpol":<Integer_value>,

"hits":<Integer_value>,
```

```
"priority":<Integer_value>,

"gotopriorityexpression":<String_value>,

"labeltype":<String_value>,

"invoke_labelname":<String_value>,

"flowtype":<Integer_value>,

"description":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/cmppolicylabel? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "cmppolicylabel": [ { "__count": "#no"} ] }
```

cmppolicylabel_binding

Binding object which returns the resources bound to cmppolicylabel.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
labelname	<String>	Read-write	Name of the HTTP compression policy label for which to display details. Minimum length = 1
cmppolicylabel_policybinding_binding	<cmppolicylabel_policybinding_binding[]>	Read-only	policybinding that can be bound to cmppolicylabel.
cmppolicylabel_cmppolicy_binding	<cmppolicylabel_cmppolicy_binding[]>	Read-only	cmppolicy that can be bound to cmppolicylabel.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.
- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of

creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/cmppolicylabel_binding/ labelname_value<String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "cmppolicylabel_binding": [ {

"labelname":<String_value>,

"cmppolicylabel_cmppolicy_binding":<cmppolicylabel_cmppolicy_binding[]_val
ue>,

"cmppolicylabel_policybinding_binding":<cmppolicylabel_policybinding_bindi
```

```
ng[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/cmppolicylabel_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/cmppolicylabel_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "cmppolicylabel_binding": [ {

"labelname":<String_value>,

"cmppolicylabel_cmppolicy_binding":<cmppolicylabel_cmppolicy_binding[]_val
ue>,

"cmppolicylabel_policybinding_binding":<cmppolicylabel_policybinding_bindi
ng[]_value>

}]}
```

cmppolicylabel_cmppolicy_binding

Binding object showing the cmppolicy that can be bound to cmppolicylabel.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
priority	<Integer>	Read-write	Specifies the priority of the policy.
labeltype	<String>	Read-write	Type of policy label invocation. Possible values = reqvserver, resvserver, policylabel
labelname	<String>	Read-write	Name of the HTTP compression policy label to which to bind the policy. Minimum length = 1
invoke_labelname	<String>	Read-write	Name of the label to invoke if the current policy evaluates to TRUE.
policyname	<String>	Read-write	The compression policy name.
invoke	<Boolean>	Read-write	Invoke policies bound to a virtual server or a user-defined policy label. After the invoked policies are evaluated, the flow

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			returns to the policy with the next higher priority number in the original label.
gotopriorityexpression	<String>	Read-write	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/cmppolicylabel_cmppolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"cmppolicylabel_cmppolicy_binding":{

<b>"labelname":<String_value>,

</b><b>"policyname":<String_value>,

</b><b>"priority":<Integer_value>,

</b>"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>,

"labeltype":<String_value>,

"invoke_labelname":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/cmppolicylabel_cmppolicy_binding/ labelname_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ cmppolicylabel_cmppolicy_binding/ labelname_value<String> ? **args= policyname:<String_value>, priority: <Integer_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/cmppolicylabel_cmppolicy_binding/ labelname_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ cmppolicylabel_cmppolicy_binding/ labelname_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of cmppolicylabel_cmppolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/cmppolicylabel_cmppolicy_binding/ labelname_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the cmppolicylabel_cmppolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "cmppolicylabel_cmppolicy_binding": [ {

"priority":<Integer_value>,

"labeltype":<String_value>,

"labelname":<String_value>,

"invoke_labelname":<String_value>,

"policyname":<String_value>,

"invoke":<Boolean_value>,

"gotopriorityexpression":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/cmppolicylabel_cmppolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/cmppolicylabel_cmppolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "cmppolicylabel_cmppolicy_binding": [ {

"priority":<Integer_value>,

"labeltype":<String_value>,

"labelname":<String_value>,

"invoke_labelname":<String_value>,

"policyname":<String_value>,

"invoke":<Boolean_value>,

"gotopriorityexpression":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/cmppolicylabel_cmppolicy_binding/labelname_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"cmppolicylabel_cmppolicy_binding": [ { "__count": "#no"} ] }
```

cmppolicylabel_policybinding_binding

Binding object showing the policybinding that can be bound to cmppolicylabel.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
labelname	<String>	Read-write	Name of the HTTP compression policy label to which to bind the policy. Minimum length = 1
priority	<Integer>	Read-write	Specifies the priority of the policy.
labeltype	<String>	Read-write	Type of policy label invocation. Possible values = reqvserver, resvserver, policylabel

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
invoke_labelname	<String>	Read-write	Name of the label to invoke if the current policy evaluates to TRUE.
policyname	<String>	Read-write	The compression policy name.
invoke	<Boolean>	Read-write	Invoke policies bound to a virtual server or a user-defined policy label. After the invoked policies are evaluated, the flow returns to the policy with the next higher priority number in the original label.
gotopriorityexpression	<String>	Read-write	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/cmppolicylabel_policybinding_binding/ labelname_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ cmppolicylabel_policybinding_binding/ labelname_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of cmppolicylabel_policybinding_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/cmppolicylabel_policybinding_binding/ labelname_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the cmppolicylabel_policybinding_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "cmppolicylabel_policybinding_binding": [ {

"labelname":<String_value>,

"priority":<Integer_value>,

"labeltype":<String_value>,

"invoke_labelname":<String_value>,

"policyname":<String_value>,

"invoke":<Boolean_value>,

"gotopriorityexpression":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/cmppolicylabel_policybinding_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/cmppolicylabel_policybinding_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "cmppolicylabel_policybinding_binding": [ {

"labelname":<String_value>,

"priority":<Integer_value>,

"labeltype":<String_value>,

"invoke_labelname":<String_value>,

"policyname":<String_value>,

"invoke":<Boolean_value>,

"gotopriorityexpression":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/cmppolicylabel_policybinding_binding/labelname_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"cmppolicylabel_policybinding_binding": [ { "__count": "#no"} ] }
```

contentinspection

CI

Content Inspection

NAME	DESCRIPTION
contentinspectionaction	Configuration for Content Inspection action
contentinspectioncallout	Configuration for Content Inspection callout
contentinspectionglobal_binding	Binding object showing the resources that can be bound to contentinspectionglobal
contentinspectionglobal_contentinspectionpolicy_binding	Binding object showing the contentinspectionpolicy that can be bound to contentinspectionglobal
contentinspectionparameter	Configuration for Contentinspection parameter

NAME	DESCRIPTION
contentinspectionpolicy	Configuration for ContentInspection policy
contentinspectionpolicy_binding	Binding object showing the resources that can be bound to contentinspectionpolicy
contentinspectionpolicy_contentinspectionglobal_binding	Binding object showing the contentinspectionglobal that can be bound to contentinspectionpolicy
contentinspectionpolicy_contentinspectionpolicylabel_binding	Binding object showing the contentinspectionpolicylabel that can be bound to contentinspectionpolicy
contentinspectionpolicy_csvserver_binding	Binding object showing the csvserver that can be bound to contentinspectionpolicy
contentinspectionpolicy_lbvserver_binding	Binding object showing the lbvserver that can be bound to contentinspectionpolicy
contentinspectionpolicylabel	Configuration for ContentInspection policy label
contentinspectionpolicylabel_binding	Binding object showing the resources that can be bound to contentinspectionpolicylabel
contentinspectionpolicylabel_contentinspectionpolicy_binding	Binding object showing the contentinspectionpolicy that can be bound to contentinspectionpolicylabel
contentinspectionpolicylabel_policybinding_binding	Binding object showing the policybinding that can be bound to contentinspectionpolicylabel

NAME	DESCRIPTION
contentinspectionprofile	Configuration for ContentInspection profile
contentinspectionwasmprofile	Configuration for WASM profile

contentinspectionaction

Configuration for Content Inspection action resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the remote service action. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters.
type	<String>	Read-write	Type of operation this action is going to perform. following actions are available to configure: * ICAP - forward the incoming request or response to an

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			ICAP server for modification. * INLINEINSPECTION - forward the incoming or outgoing packets to IPS server for Intrusion Prevention. * MIRROR - Forwards cloned packets for Intrusion Detection. * NOINSPECTION - This does not forward incoming and outgoing packets to the Inspection device. * NSTRACE - capture current and further incoming packets on this transaction. Possible values = ICAP, INLINEINSPECTION, MIRROR, NOINSPECTION, WASM

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
servername	<String>	Read-write	Name of the LB vserver or service. Minimum length = 1 Maximum length = 127
serverip	<String>	Read-write	IP address of remoteService. Minimum length = 1
serverport	<Integer>	Read-write	Port of remoteService. Default value: 1344 Minimum value = 1 Maximum value = 65535
icapprofilename	<String>	Read-write	Name of the ICAP profile to be attached to the contentInspection action. Minimum length = 1 Maximum length = 127
wasmprofilename	<String>	Read-write	Name of the CI WASM profile to be attached to the contentInspection action. Minimum length = 1 Maximum length = 127

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ifserverdown	<String>	Read-write	Name of the action to perform if the Vserver representing the remote service is not UP. This is not supported for NOINSPECTION Type. The Supported actions are: * RESET - Reset the client connection by closing it. The client program, such as a browser, will handle this and may inform the user. The client may then resend the request if desired. * DROP - Drop the request without sending a response to the user. * CONTINUE - It bypasses the ContentIsnpection and Continues/ resumes the Traffic-Flow to Client/ Server. Default value: RESET

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = CONTINUE, DROP, RESET
reqtimeout	<Integer>	Read-only	Time, in seconds, within which the remote service request must complete. This is not supported for NOINSPECTION action type. If the request does not complete within this time, the specified request timeout action is executed. Zero disables the timeout. Default value: 0 Minimum value = 0 Maximum value = 86400
reqtimeoutaction	<String>	Read-only	Name of the action to perform if the Vserver representing the remote service does not respond. This is not supported for NOINSPECTION action type. There are also some built-in actions which can be used. These are: * RESET - Reset the client connection by

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			closing it. The client program, such as a browser, will handle this and may inform the user. The client may then resend the request if desired. * DROP - Drop the request without sending a response to the user. Default value: BYPASS Possible values = BYPASS, DROP, RESET
hits	<Integer>	Read-only	The number of times the action has been taken.
referencecount	<Integer>	Read-only	The number of references to the action.
undefhits	<Integer>	Read-only	The number of times the action resulted in UNDEF.
builtin	<String[]>	Read-only	Flag to determine whether contentinspection action is built-in or not.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL
feature	<String>	Read-only	The feature to be checked while applying this config.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- GET (ALL)
- GET
- COUNT
- UPDATE
- UNSET
- DELETE

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of

creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/contentinspectionaction **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"contentinspectionaction":{

<b>"name":<String_value>,

</b><b>"type":<String_value>,

</b>"servername":<String_value>,

"serverip":<String_value>,

"serverport":<Integer_value>,

"icapprofilename":<String_value>,

"wasmprofilename":<String_value>,

"ifserverdown":<String_value>
```

```
}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/contentinspectionaction **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"contentinspectionaction":{

<b>"name":<String_value>,

</b>"servername":<String_value>,

"serverip":<String_value>,

"serverport":<Integer_value>,

"icapprofilename":<String_value>,

"wasmprofilename":<String_value>,

"ifserverdown":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/contentinspectionaction? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"contentinspectionaction":{

<b>"name":<String_value>,

</b>"serverport":true,

"ifserverdown":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/contentinspectionaction/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/contentinspectionaction **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/contentinspectionaction? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/contentinspectionaction? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of contentinspectionaction resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/contentinspectionaction? **view=summary**

Use this query-parameter to get the summary output of contentinspectionaction resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/contentinspectionaction? **pagesize=#no;pageno=#no**

Use this query-parameter to get the contentinspectionaction resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "contentinspectionaction": [ {

"name":<String_value>,

"type":<String_value>,

"servername":<String_value>,

"serverip":<String_value>,

"serverport":<Integer_value>,

"icapprofilename":<String_value>,

"wasmprofilename":<String_value>,

"ifserverdown":<String_value>,

"reqtimeout":<Integer_value>,

"reqtimeoutaction":<String_value>,

"hits":<Integer_value>,

"referencecount":<Integer_value>,

"undefhits":<Integer_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/contentinspectionaction/ name_value<String>
Query-parameters: attrs http:// <netscaler-ip-address> /nitro/v1/config/contentinspectionaction/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/contentinspectionaction/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of contentinspectionaction resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "contentinspectionaction": [ {

"name":<String_value>,

"type":<String_value>,

"servername":<String_value>,

"serverip":<String_value>,

"serverport":<Integer_value>,

"icapprofilename":<String_value>,

"wasmprofilename":<String_value>,
```

```
"ifserverdown":<String_value>,

"reqtimeout":<Integer_value>,

"reqtimeoutaction":<String_value>,

"hits":<Integer_value>,

"referencecount":<Integer_value>,

"undefhits":<Integer_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/contentinspectionaction? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "contentinspectionaction": [ { "__count": "#no"} ] }
```

contentinspectioncallout

Configuration for Content Inspection callout resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the Content Inspection callout. Not case sensitive. Must begin with an ASCII letter or underscore (_) character, and must consist only of ASCII alphanumeric or underscore characters. Must not begin with 're' or 'xp' or be a word reserved for use as an expression qualifier prefix (such as HTTP) or enumeration value (such as ASCII). Must not be the name of an existing named expression, pattern set, dataset, stringmap, or callout. Minimum length = 1
type	<String>	Read-write	Type of the Content Inspection callout. It

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			must be one of the following: * ICAP - Sends ICAP request to the configured ICAP server. Possible values = ICAP
profilename	<String>	Read-write	Name of the Content Inspection profile. The type of the configured profile must match the type specified using -type argument. Minimum length = 1 Maximum length = 127
servername	<String>	Read-write	Name of the load balancing or content switching virtual server or service to which the Content Inspection request is issued. Mutually exclusive with server IP address and port parameters. The service type must be TCP or SSL_TCP. If there are vservers and services with the same name, then vserver is selected. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum length = 127
serverip	<String>	Read-write	IP address of Content Inspection server. Mutually exclusive with the server name parameter. Minimum length = 1
serverport	<Integer>	Read-write	Port of the Content Inspection server. Default value: 1344 Minimum value = 1 Maximum value = 65535
returntype	<String>	Read-write	Type of data that the target callout agent returns in response to the callout. Available settings function as follows: * TEXT - Treat the returned value as a text string. * NUM - Treat the returned value as a number. * BOOL - Treat the returned value as a Boolean value.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Note: You cannot change the return type after it is set. Possible values = BOOL, NUM, TEXT
resultexpr	<String>	Read-write	Expression that extracts the callout results from the response sent by the CI callout agent. Must be a response based expression, that is, it must begin with ICAP.RES. The operations in this expression must match the return type. For example, if you configure a return type of TEXT, the result expression must be a text based expression, as in the following example: icap.res.header("ISTag"). Minimum length = 1
comment	<String>	Read-write	Any comments to preserve information about this Content Inspection callout.
hits	<Integer>	Read-only	Total hits.
undefhits	<Integer>	Read-only	Total undefs.
undefreason	<String>	Read-only	Reason for last undef.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = Failed to add service, Vserver not found, Not a HTTP or SSL vserver, Generated callout request is invalid, Content-Length header not found in callout request, Not enough space to put Content-Length value, Config incomplete, Server is DOWN, Creating callout connection failed, No memory to generate callout request packets, No memory to create callout task, No memory to create callout async, Callout request expression undef, No callout response expression, Skipped callout response eval, Callout response pixl init undef, Callout response expression undef
_nextgenapiresource	<String>	Read-only	.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/contentinspectioncallout **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"contentinspectioncallout":{

<b>"name":<String_value>,

</b><b>"type":<String_value>,

</b>"profilename":<String_value>,

"servername":<String_value>,

"serverip":<String_value>,

"serverport":<Integer_value>,

<b>"returntype":<String_value>,

</b><b>"resultexpr":<String_value>,

</b>"comment":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/contentinspectioncallout/ name_value<String>
HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/contentinspectioncallout **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"contentinspectioncallout":{

<b>"name":<String_value>,

</b>"servername":<String_value>,

"serverip":<String_value>,

"serverport":<Integer_value>,

"profilename":<String_value>,

"returntype":<String_value>,

"resultexpr":<String_value>,

"comment":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/contentinspectioncallout? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"contentinspectioncallout":{

<b>"name":<String_value>,

</b>"serverport":true,

"comment":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/contentinspectioncallout **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/contentinspectioncallout? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/contentinspectioncallout? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of contentinspectioncallout resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/contentinspectioncallout? **view=summary**

Use this query-parameter to get the summary output of contentinspectioncallout resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/contentinspectioncallout? **pagesize=#no;pageno=#no**

Use this query-parameter to get the contentinspectioncallout resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "contentinspectioncallout": [ {

"name":<String_value>,

"type":<String_value>,

"profilename":<String_value>,
```

```
"servername":<String_value>,

"serverip":<String_value>,

"serverport":<Integer_value>,

"returntype":<String_value>,

"resultexpr":<String_value>,

"hits":<Integer_value>,

"undefhits":<Integer_value>,

"undefreason":<String_value>,

"comment":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/contentinspectioncallout/ name_value<String>
Query-parameters: attrs http:// <netscaler-ip-address> /nitro/v1/config/contentinspectioncallout/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/contentinspectioncallout/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of contentinspectioncallout resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "contentinspectioncallout": [ {

"name":<String_value>,

"type":<String_value>,

"profilename":<String_value>,

"servername":<String_value>,

"serverip":<String_value>,

"serverport":<Integer_value>,

"returntype":<String_value>,

"resultexpr":<String_value>,

"hits":<Integer_value>,

"undefhits":<Integer_value>,

"undefreason":<String_value>,

"comment":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/contentinspectioncallout? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "contentinspectioncallout": [ { "__count": "#no"} ] }
```

contentinspectionglobal_binding

Binding object which returns the resources bound to contentinspectionglobal.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
contentinspectionglobal_contentinspectionpolicy_binding	<contentinspectionglobal_contentinspectionpolicy_binding[]>	Read-write	contentinspectionpolicy that can be bound to contentinspectionglobal.

Operations

(click to see Properties)

- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/contentinspectionglobal_binding

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "contentinspectionglobal_binding": [ {

"contentinspectionglobal_contentinspectionpolicy_binding":<contentinspectionglobal_contentinspectionpolicy_binding[]_value>

}]}
```

contentinspectionglobal_contentinspectionpolicy_binding

Binding object showing the contentinspectionpolicy that can be bound to contentinspectionglobal.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
priority	<Integer>	Read-write	Specifies the priority of the policy.
labeltype	<String>	Read-write	Type of invocation. Available settings function as follows: * reqvserver - Forward the request to the specified request virtual server. * resvserver - Forward

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			the response to the specified response virtual server. * policylabel - Invoke the specified policy label. Possible values = reqvserver, resvserver, policylabel
labelname	<String>	Read-write	* If labelType is policylabel, name of the policy label to invoke. * If labelType is reqvserver or resvserver, name of the virtual server to which to forward the request of response.
type	<String>	Read-write	The bindpoint to which to policy is bound. Possible values = REQ_OVERRIDE, REQ_DEFAULT, RES_OVERRIDE, RES_DEFAULT
invoke	<Boolean>	Read-write	Terminate evaluation of policies bound to the current policy label, and then forward the request to the specified virtual server or evaluate the specified policy label.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
gotopriorityexpression	<String>	Read-write	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
globalbindtype	<String>	Read-write	. Default value: SYSTEM_GLOBAL Possible values = SYSTEM_GLOBAL, VPN_GLOBAL, RNAT_GLOBAL, APPFW_GLOBAL, TM_GLOBAL
policyname	<String>	Read-write	Name of the contentInspection policy.
numpol	<Integer>	Read-only	The number of policies bound to the bindpoint.
flowtype	<Integer>	Read-only	flowtype of the bound contentInspection policy.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE

- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/contentinspectionglobal_contentinspectionpolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"contentinspectionglobal_contentinspectionpolicy_binding":{

<b>"policyname":<String_value>,

</b><b>"priority":<Integer_value>,

</b>"gotopriorityexpression":<String_value>,

"type":<String_value>,

"invoke":<Boolean_value>,

"labeltype":<String_value>,

"labelname":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/ contentinspectionglobal_contentinspectionpolicy_binding **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/contentinspectionglobal_contentinspectionpolicy_binding? **args= policyname:<String_value>, type: <String_value> ,priority: <Integer_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/ contentinspectionglobal_contentinspectionpolicy_binding **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/contentinspectionglobal_contentinspectionpolicy_binding? **args=type: <String_value>**

Use this query-parameter to get contentinspectionglobal_contentinspectionpolicy_binding resources based on additional properties.

filter http:// <netscaler-ip-address> /nitro/v1/config/ contentinspectionglobal_contentinspectionpolicy_binding? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of contentinspectionglobal_contentinspectionpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ contentinspectionglobal_contentinspectionpolicy_binding? **pagesize=#no;pageno=#no**

Use this query-parameter to get the contentinspectionglobal_contentinspectionpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "contentinspectionglobal_contentinspectionpolicy_binding": [ {

"priority":<Integer_value>,

"labeltype":<String_value>,

"labelname":<String_value>,

"type":<String_value>,

"invoke":<Boolean_value>,

"gotopriorityexpression":<String_value>,

"globalbindtype":<String_value>,

"policyname":<String_value>,

"numpol":<Integer_value>,

"flowtype":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/ contentinspectionglobal_contentinspectionpolicy_binding? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "contentinspectionglobal_contentinspectionpolicy_binding":
[ { "__count": "#no"} ] }
```

contentinspectionparameter

Configuration for Contentinspection parameter resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
undefaction	<String>	Read-write	Action to perform if the result of policy evaluation is undefined (UNDEF). An UNDEF event indicates an error condition in evaluating the expression. Available settings function as follows: * NOINSPECTION - Do not Inspect the traffic. * RESET - Reset the connection and notify the user's browser, so that the user can resend the request. * DROP - Drop the message without

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			sending a response to the user. Default value: "NOINSPECTION"
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- UPDATE
- UNSET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/contentinspectionparameter **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"contentinspectionparameter":{

"undefaction":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/contentinspectionparameter? **action=unset** **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"contentinspectionparameter":{

"undefaction":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/contentinspectionparameter **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "contentinspectionparameter": [ {

"undefaction":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

contentinspectionpolicy

Configuration for ContentInspection policy resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the contentInspection policy. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Can be changed after the contentInspection policy is added. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my contentInspection policy" or 'my contentInspection policy').

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
rule	<String>	Read-write	Expression that the policy uses to determine whether to execute the specified action.
action	<String>	Read-write	Name of the contentInspection action to perform if the request matches this contentInspection policy. There are also some built-in actions which can be used. These are: * NOINSPECTION - Send the request from the client to the server or response from the server to the client without sending it to Inspection device for Content Inspection. * RESET - Resets the client connection by closing it. The client program, such as a browser, will handle this and may inform the user. The client may then resend

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			the request if desired. * DROP - Drop the request without sending a response to the user.
undefaction	<String>	Read-write	Action to perform if the result of policy evaluation is undefined (UNDEF). An UNDEF event indicates an internal error condition. Only the above built-in actions can be used.
comment	<String>	Read-write	Any type of information about this contentInspection policy.
logaction	<String>	Read-write	Name of the messagelog action to use for requests that match this policy.
newname	<String>	Read-write	New name for the contentInspection policy. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space ( ), at (@), equals (=), colon (:),

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			and underscore characters. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my contentInspection policy" or 'my contentInspection policy'). Minimum length = 1
hits	<Integer>	Read-only	Number of hits.
undefhits	<Integer>	Read-only	Number of policy UNDEF hits.
builtin	<String[]>	Read-only	Flag to determine if contentInspection policy is built-in or not. Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL
feature	<String>	Read-only	The feature to be checked while applying this config.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT
- RENAME

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/contentinspectionpolicy **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"contentinspectionpolicy":{

<b>"name":<String_value>,

</b><b>"rule":<String_value>,

</b><b>"action":<String_value>,

</b>"undefaction":<String_value>,

"comment":<String_value>,

"logaction":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/contentinspectionpolicy/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/contentinspectionpolicy **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"contentinspectionpolicy":{

<b>"name":<String_value>,

</b>"rule":<String_value>,

"action":<String_value>,

"undefaction":<String_value>,

"comment":<String_value>,

"logaction":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/contentinspectionpolicy? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"contentinspectionpolicy":{

<b>"name":<String_value>,

</b>"undefaction":true,

"comment":true,

"logaction":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

RENAME

URL: http:// <netscaler-ip-address> /nitro/v1/config/contentinspectionpolicy? **action=rename**
HTTP Method: POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"contentinspectionpolicy":{

<b>"name":<String_value>,

</b><b>"newname":<String_value>
```

```
</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/contentinspectionpolicy **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/contentinspectionpolicy? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/contentinspectionpolicy? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of contentinspectionpolicy resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/contentinspectionpolicy? **view=summary**

Use this query-parameter to get the summary output of contentinspectionpolicy resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/contentinspectionpolicy? **pagesize=#no;pageno=#no**

Use this query-parameter to get the contentinspectionpolicy resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "contentinspectionpolicy": [ {

"name":<String_value>,

"rule":<String_value>,

"action":<String_value>,

"undefaction":<String_value>,

"hits":<Integer_value>,

"undefhits":<Integer_value>,

"comment":<String_value>,

"logaction":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/contentinspectionpolicy/ name_value<String>
Query-parameters: attrs http:// <netscaler-ip-address> /nitro/v1/config/contentinspectionpolicy/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/contentinspectionpolicy/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of contentinspectionpolicy resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "contentinspectionpolicy": [ {

"name":<String_value>,

"rule":<String_value>,

"action":<String_value>,

"undefaction":<String_value>,

"hits":<Integer_value>,

"undefhits":<Integer_value>,

"comment":<String_value>,

"logaction":<String_value>,
```

```
"builtin":<String[]_value>,

"feature":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/contentinspectionpolicy? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "contentinspectionpolicy": [ { "__count": "#no"} ] }
```

contentinspectionpolicy_binding

Binding object which returns the resources bound to contentinspectionpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the contentInspection policy for which to display settings.
contentinspectionpolicy_contentinspectionpolicylabel_binding	<contentinspectionpolicy_contentinspectionpolicylabel_binding[]>	Read-only	contentinspectionpolicylabel that can be bound to contentinspectionpolicy.
contentinspectionpolicy_contentinspectionglobal_binding	<contentinspectionpolicy_contentinspectionglobal_binding[]>	Read-only	contentinspectionglobal that can be bound to contentinspectionpolicy.
contentinspectionpolicy_csvserver_binding	<contentinspectionpolicy_csvserver_binding[]>	Read-only	csvserver that can be bound to contentinspectionpolicy.
contentinspectionpolicy_lbvserver_binding	<contentinspectionpolicy_lbvserver_binding[]>	Read-only	lbvserver that can be bound to contentinspectionpolicy.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/contentinspectionpolicy_binding/ name_value<String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "contentinspectionpolicy_binding": [ {

"name":<String_value>,
```

```
"contentinspectionpolicy_csvserver_binding":<contentinspectionpolicy_csvserver_binding[]_value>,

"contentinspectionpolicy_contentinspectionglobal_binding":<contentinspectionpolicy_contentinspectionglobal_binding[]_value>,

"contentinspectionpolicy_lbvserver_binding":<contentinspectionpolicy_lbvserver_binding[]_value>,

"contentinspectionpolicy_contentinspectionpolicylabel_binding":<contentinspectionpolicy_contentinspectionpolicylabel_binding[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/contentinspectionpolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/contentinspectionpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "contentinspectionpolicy_binding": [ {

"name":<String_value>,

"contentinspectionpolicy_csvserver_binding":<contentinspectionpolicy_csvserver_binding[]_value>,

"contentinspectionpolicy_contentinspectionglobal_binding":<contentinspectionpolicy_contentinspectionglobal_binding[]_value>,

"contentinspectionpolicy_lbvserver_binding":<contentinspectionpolicy_lbvserver_binding[]_value>,

"contentinspectionpolicy_contentinspectionpolicylabel_binding":<contentinspectionpolicy_contentinspectionpolicylabel_binding[]_value>

}]}
```

contentinspectionpolicy_contentinspectionglobal_binding

Binding object showing the contentinspectionglobal that can be bound to contentinspectionpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the contentInspection policy for which to display settings.
boundto	<String>	Read-write	Location where policy is bound.
labelname	<String>	Read-only	Name of the label to invoke if the current policy rule evaluates to TRUE.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
gotopriorityexpression	<String>	Read-only	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
activepolicy	<Integer>	Read-only	Indicates whether policy is bound or not.
labeltype	<String>	Read-only	Type of policy label invocation. Possible values = reqvserver, resvserver, policylabel
priority	<Integer>	Read-only	Specifies the priority of the policy.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/ contentinspectionpolicy_contentinspectionglobal_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ contentinspectionpolicy_contentinspectionglobal_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of contentinspectionpolicy_contentinspectionglobal_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ contentinspectionpolicy_contentinspectionglobal_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the contentinspectionpolicy_contentinspectionglobal_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "contentinspectionpolicy_contentinspectionglobal_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"labelname":<String_value>,

"gotopriorityexpression":<String_value>,

"activepolicy":<Integer_value>,

"labeltype":<String_value>,

"priority":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/ contentinspectionpolicy_contentinspectionglobal_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ contentinspectionpolicy_contentinspectionglobal_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "contentinspectionpolicy_contentinspectionglobal_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"labelname":<String_value>,

"gotopriorityexpression":<String_value>,

"activepolicy":<Integer_value>,

"labeltype":<String_value>,

"priority":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/ contentinspectionpolicy_contentinspectionglobal_binding/ name_value<String> ? **count=yes**
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"contentinspectionpolicy_contentinspectionglobal_binding": [ { "__count":
"#no"} ] }
```

contentinspectionpolicy_contentinspectionpolicylabel_binding

Binding object showing the contentinspectionpolicylabel that can be bound to contentinspectionpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the contentInspection policy for which to display settings.
boundto	<String>	Read-write	Location where policy is bound.
priority	<Integer>	Read-only	Specifies the priority of the policy.
labeltype	<String>	Read-only	Type of policy label invocation.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = reqvserver, resvserver, policylabel
activepolicy	<Integer>	Read-only	Indicates whether policy is bound or not.
gotopriorityexpression	<String>	Read-only	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
labelname	<String>	Read-only	Name of the label to invoke if the current policy rule evaluates to TRUE.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/ contentinspectionpolicy_contentinspectionpolicylabel_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ contentinspectionpolicy_contentinspectionpolicylabel_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of contentinspectionpolicy_contentinspectionpolicylabel_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ contentinspectionpolicy_contentinspectionpolicylabel_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the contentinspectionpolicy_contentinspectionpolicylabel_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "contentinspectionpolicy_contentinspectionpolicylabel_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"priority":<Integer_value>,

"labeltype":<String_value>,

"activepolicy":<Integer_value>,

"gotopriorityexpression":<String_value>,

"labelname":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/ contentinspectionpolicy_contentinspectionpolicylabel_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ contentinspectionpolicy_contentinspectionpolicylabel_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "contentinspectionpolicy_contentinspectionpolicylabel_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"priority":<Integer_value>,

"labeltype":<String_value>,

"activepolicy":<Integer_value>,

"gotopriorityexpression":<String_value>,

"labelname":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/ contentinspectionpolicy_contentinspectionpolicylabel_binding/ name_value<String> ? **count=yes**
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"contentinspectionpolicy_contentinspectionpolicylabel_binding":
[ { "__count": "#no"} ] }
```

contentinspectionpolicy_csvserver_binding

Binding object showing the csvserver that can be bound to contentinspectionpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
boundto	<String>	Read-write	Location where policy is bound.
name	<String>	Read-write	Name of the contentInspection policy for which to display settings.
priority	<Integer>	Read-only	Specifies the priority of the policy.
labeltype	<String>	Read-only	Type of policy label invocation. Possible values = reqvserver,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			resvserver, policylabel
activepolicy	<Integer>	Read-only	Indicates whether policy is bound or not.
gotopriorityexpression	<String>	Read-only	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
labelname	<String>	Read-only	Name of the label to invoke if the current policy rule evaluates to TRUE.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/contentinspectionpolicy_csvserver_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ contentinspectionpolicy_csvserver_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of contentinspectionpolicy_csvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ contentinspectionpolicy_csvserver_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the contentinspectionpolicy_csvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "contentinspectionpolicy_csvserver_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"priority":<Integer_value>,

"labeltype":<String_value>,

"activepolicy":<Integer_value>,

"gotopriorityexpression":<String_value>,

"labelname":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/contentinspectionpolicy_csvserver_binding
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/contentinspectionpolicy_csvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "contentinspectionpolicy_csvserver_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"priority":<Integer_value>,

"labeltype":<String_value>,

"activepolicy":<Integer_value>,

"gotopriorityexpression":<String_value>,

"labelname":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/contentinspectionpolicy_csvserver_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"contentinspectionpolicy_csvserver_binding": [ { "__count": "#no"} ] }
```

contentinspectionpolicy_lbvserver_binding

Binding object showing the lbvserver that can be bound to contentinspectionpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the contentInspection policy for which to display settings.
boundto	<String>	Read-write	Location where policy is bound.
labeltype	<String>	Read-only	Type of policy label invocation. Possible values = reqvserver, resvserver, policylabel
priority	<Integer>	Read-only	Specifies the priority of the policy.
labelname	<String>	Read-only	Name of the label to invoke if the current

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			policy rule evaluates to TRUE.
gotopriorityexpression	<String>	Read-only	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
activepolicy	<Integer>	Read-only	Indicates whether policy is bound or not.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/contentinspectionpolicy_lbvserver_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ contentinspectionpolicy_lbvserver_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of contentinspectionpolicy_lbvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ contentinspectionpolicy_lbvserver_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the contentinspectionpolicy_lbvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "contentinspectionpolicy_lbvserver_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"labelname":<String_value>,

"gotopriorityexpression":<String_value>,

"activepolicy":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/contentinspectionpolicy_lbvserver_binding
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ contentinspectionpolicy_lbvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "contentinspectionpolicy_lbvserver_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"labelname":<String_value>,

"gotopriorityexpression":<String_value>,

"activepolicy":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/contentinspectionpolicy_lbvserver_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"contentinspectionpolicy_lbvserver_binding": [ { "__count": "#no"} ] }
```

contentinspectionpolicylabel

Configuration for ContentInspection policy label resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
labelname	<String>	Read-write	Name for the contentInspection policy label. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after the contentInspection policy label is added. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			single quotation marks (for example, "my contentInspection policy label" or 'my contentInspection policy label').
type	<String>	Read-write	Type of packets (request or response packets) against which to match the policies bound to this policy label. Possible values = REQ, RES
comment	<String>	Read-write	Any comments to preserve information about this contentInspection policy label.
newname	<String>	Read-write	New name for the contentInspection policy label. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space ( ), at (@), equals (=), colon (:),

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			and underscore characters. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my policy label" or 'my policy label'). Minimum length = 1
numpol	<Integer>	Read-only	Number of polices bound to label.
hits	<Integer>	Read-only	Number of times policy label was invoked.
priority	<Integer>	Read-only	Specifies the priority of the policy.
gotopriorityexpression	<String>	Read-only	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
labeltype	<String>	Read-only	Type of invocation. Available settings function as follows:

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			* reqvserver - Forward the request to the specified request virtual server. * resvserver - Forward the response to the specified response virtual server. * policylabel - Invoke the specified policy label. Possible values = reqvserver, resvserver, policylabel
invoke_labelname	<String>	Read-only	* If labelType is policylabel, name of the policy label to invoke. * If labelType is reqvserver or resvserver, name of the virtual server to which to forward the request or response.
flowtype	<Integer>	Read-only	Flowtype of the bound contentInspection policy.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
isdefault	<Boolean>	Read-only	A value of true is returned if it is a default cipolicylabel.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET (ALL)
- GET
- COUNT
- RENAME

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/contentinspectionpolicylabel **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"contentinspectionpolicylabel":{

<b>"labelname":<String_value>,

</b><b>"type":<String_value>,

</b>"comment":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/contentinspectionpolicylabel/labelname_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

RENAME

URL: http:// <netscaler-ip-address> /nitro/v1/config/contentinspectionpolicylabel? **action=rename**
HTTP Method: POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"contentinspectionpolicylabel":{

<b>"labelname":<String_value>,

</b><b>"newname":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/contentinspectionpolicylabel **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/contentinspectionpolicylabel? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/contentinspectionpolicylabel? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of contentinspectionpolicylabel resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/contentinspectionpolicylabel? **view=summary**

Use this query-parameter to get the summary output of contentinspectionpolicylabel resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/contentinspectionpolicylabel? **pagesize=#no;pageno=#no**

Use this query-parameter to get the contentinspectionpolicylabel resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "contentinspectionpolicylabel": [ {

"labelname":<String_value>,

"type":<String_value>,

"numpol":<Integer_value>,

"hits":<Integer_value>,

"priority":<Integer_value>,

"gotopriorityexpression":<String_value>,
```

```
"labeltype":<String_value>,

"invoke_labelname":<String_value>,

"flowtype":<Integer_value>,

"isdefault":<Boolean_value>,

"comment":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/contentinspectionpolicylabel/ labelname_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/ contentinspectionpolicylabel/ labelname_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/contentinspectionpolicylabel/ labelname_value<String> ? **view=summary**

Use this query-parameter to get the summary output of contentinspectionpolicylabel resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "contentinspectionpolicylabel": [ {

"labelname":<String_value>,

"type":<String_value>,

"numpol":<Integer_value>,

"hits":<Integer_value>,

"priority":<Integer_value>,

"gotopriorityexpression":<String_value>,

"labeltype":<String_value>,

"invoke_labelname":<String_value>,

"flowtype":<Integer_value>,

"isdefault":<Boolean_value>,

"comment":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/contentinspectionpolicylabel? **count=yes**
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "contentinspectionpolicylabel": [ { "__count": "#no"} ] }
```

contentinspectionpolicylabel_binding

Binding object which returns the resources bound to contentinspectionpolicylabel.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
labelname	<String>	Read-write	Name of the contentInspection policy label.
contentinspectionpolicylabel_contentinspectionpolicy_binding	<contentinspectionpolicylabel_contentinspectionpolicy_binding[]>	Read-only	contentinspectionpolicy that can be bound to contentinspectionpolicylabel.
contentinspectionpolicylabel_policybinding_binding	<contentinspectionpolicylabel_policybinding_binding[]>	Read-only	policybinding that can be bound to contentinspectionpolicylabel.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/contentinspectionpolicylabel_binding/labelname_value<String>

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "contentinspectionpolicylabel_binding": [ {

"labelname":<String_value>,

"contentinspectionpolicylabel_policybinding_binding":<contentinspectionpol
icylabel_policybinding_binding[]_value>,

"contentinspectionpolicylabel_contentinspectionpolicy_binding":<contentins
pectionpolicylabel_contentinspectionpolicy_binding[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/contentinspectionpolicylabel_binding

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters:

bulkbindings

http:// <netscaler-ip-address> /nitro/v1/config/contentinspectionpolicylabel_binding?**bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "contentinspectionpolicylabel_binding": [ {

"labelname":<String_value>,

"contentinspectionpolicylabel_policybinding_binding":<contentinspectionpolicylabel_policybinding_binding[]_value>,

"contentinspectionpolicylabel_contentinspectionpolicy_binding":<contentinspectionpolicylabel_contentinspectionpolicy_binding[]_value>

}]}
```

contentinspectionpolicylabel_contentinspectionpolicy_binding

Binding object showing the contentinspectionpolicy that can be bound to contentinspectionpolicylabel.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
invoke	<Boolean>	Read-write	Suspend evaluation of policies bound to the current policy label, and then forward the request to the specified virtual server or evaluate the specified policy label.
gotopriorityexpression	<String>	Read-write	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
policyname	<String>	Read-write	Name of the contentInspection policy to bind to the policy label.
invoke_labelname	<String>	Read-write	* If labelType is policylabel, name of the policy label to invoke. * If labelType is reqvserver or resvserver, name of the virtual server to which to forward the request or response.
labelname	<String>	Read-write	Name of the contentInspection policy label to which to bind the policy.
priority	<Integer>	Read-write	Specifies the priority of the policy.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
labeltype	<String>	Read-write	Type of invocation. Available settings function as follows: * reqvserver - Forward the request to the specified request virtual server. * resvserver - Forward the response to the specified response virtual server. * policylabel - Invoke the specified policy label. Possible values = reqvserver, resvserver, policylabel
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/ contentinspectionpolicylabel_contentinspectionpolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"contentinspectionpolicylabel_contentinspectionpolicy_binding":{

<b>"labelname":<String_value>,

</b><b>"policyname":<String_value>,

</b><b>"priority":<Integer_value>,

</b>"gotopriorityexpression":<String_value>,
```

```
"invoke":<Boolean_value>,

"labeltype":<String_value>,

"invoke_labelname":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/ contentinspectionpolicylabel_contentinspectionpolicy_binding/ labelname_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ contentinspectionpolicylabel_contentinspectionpolicy_binding/ labelname_value<String> ? **args= policyname:<String_value>, priority: <Integer_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/ contentinspectionpolicylabel_contentinspectionpolicy_binding/ labelname_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ contentinspectionpolicylabel_contentinspectionpolicy_binding/ labelname_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of contentinspectionpolicylabel_contentinspectionpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ contentinspectionpolicylabel_contentinspectionpolicy_binding/ labelname_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the contentinspectionpolicylabel_contentinspectionpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "contentinspectionpolicylabel_contentinspectionpolicy_binding": [ {

"invoke":<Boolean_value>,

"gotopriorityexpression":<String_value>,

"policyname":<String_value>,

"invoke_labelname":<String_value>,

"labelname":<String_value>,

"priority":<Integer_value>,
```

```
"labeltype":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/ contentinspectionpolicylabel_contentinspectionpolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ contentinspectionpolicylabel_contentinspectionpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "contentinspectionpolicylabel_contentinspectionpolicy_binding": [ {

"invoke":<Boolean_value>,

"gotopriorityexpression":<String_value>,

"policyname":<String_value>,

"invoke_labelname":<String_value>,
```

```
"labelname":<String_value>,

"priority":<Integer_value>,

"labeltype":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/ contentinspectionpolicylabel_contentinspectionpolicy_binding/ labelname_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"contentinspectionpolicylabel_contentinspectionpolicy_binding":
[ { "__count": "#no"} ] }
```

contentinspectionpolicylabel_policybinding_binding

Binding object showing the policybinding that can be bound to contentinspectionpolicylabel.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
invoke_labelname	<String>	Read-write	* If labelType is policylabel, name of the policy label to invoke. * If labelType is reqvserver or resvserver, name of the virtual server to which to forward the request or response.
gotopriorityexpression	<String>	Read-write	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
invoke	<Boolean>	Read-write	Suspend evaluation of policies bound to the current policy label, and then forward the request to the specified virtual server or evaluate the specified policy label.
policyname	<String>	Read-write	Name of the contentInspection policy to bind to the policy label.
labelname	<String>	Read-write	Name of the contentInspection policy label to which to bind the policy.
labeltype	<String>	Read-write	Type of invocation. Available settings function as follows: *

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			reqvserver - Forward the request to the specified request virtual server. * resvserver - Forward the response to the specified response virtual server. * policylabel - Invoke the specified policy label. Possible values = reqvserver, resvserver, policylabel
priority	<Integer>	Read-write	Specifies the priority of the policy.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/ contentinspectionpolicylabel_policybinding_binding/ labelname_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ contentinspectionpolicylabel_policybinding_binding/ labelname_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of contentinspectionpolicylabel_policybinding_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ contentinspectionpolicylabel_policybinding_binding/ labelname_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the contentinspectionpolicylabel_policybinding_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "contentinspectionpolicylabel_policybinding_binding": [ {

"invoke_labelname":<String_value>,

"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>,

"policyname":<String_value>,

"labelname":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/ contentinspectionpolicylabel_policybinding_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ contentinspectionpolicylabel_policybinding_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "contentinspectionpolicylabel_policybinding_binding": [ {

"invoke_labelname":<String_value>,

"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>,

"policyname":<String_value>,

"labelname":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/ contentinspectionpolicylabel_policybinding_binding/ labelname_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"contentinspectionpolicylabel_policybinding_binding": [ { "__count":
"#no"} ] }
```

contentinspectionprofile

Configuration for ContentInspection profile resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of a ContentInspection profile. Must begin with a letter, number, or the underscore \(_\) character. Other characters allowed, after the first character, are the hyphen \(-\), period \(.\), hash \(#\), space \(\), at \(@\), colon \(:\), and equal \(=\) characters. The name of a IPS profile cannot be changed after it is created.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks \ (for example, "my ips profile" or 'my ips profile'\). Minimum length = 1 Maximum length = 127
type	<String>	Read-write	Type of ContentInspection profile. Following types are available to configure: INLINEINSPECTION : To inspect the packets/requests using IPS. MIRROR : To forward cloned packets. Possible values = InlineInspection, Mirror
ingressinterface	<String>	Read-write	Ingress interface for CI profile.It is a mandatory argument while creating an ContentInspection profile of IPS type.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ingressvlan	<Integer>	Read-write	Ingress Vlan for CI.
egressinterface	<String>	Read-write	Egress interface for CI profile.It is a mandatory argument while creating an ContentInspection profile of type INLINEINSPECTION or MIRROR.
iptunnel	<String>	Read-write	IP Tunnel for CI profile. It is used while creating a ContentInspection profile of type MIRROR when the IDS device is in a different network. Minimum length = 1 Maximum length = 31
egressvlan	<Integer>	Read-write	Egress Vlan for CI.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)

- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/contentinspectionprofile **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"contentinspectionprofile":{

<b>"name":<String_value>,

</b><b>"type":<String_value>,

</b>"ingressinterface":<String_value>,

"ingressvlan":<Integer_value>,

"egressinterface":<String_value>,

"iptunnel":<String_value>,

"egressvlan":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/contentinspectionprofile/ name_value<String>
HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/contentinspectionprofile **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"contentinspectionprofile":{

<b>"name":<String_value>,

</b>"egressinterface":<String_value>,

"ingressinterface":<String_value>,

"egressvlan":<Integer_value>,

"ingressvlan":<Integer_value>,

"iptunnel":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/contentinspectionprofile? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"contentinspectionprofile":{

<b>"name":<String_value>,

</b>"egressvlan":true,
```

```
"ingressvlan":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/contentinspectionprofile **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/contentinspectionprofile? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/contentinspectionprofile? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of contentinspectionprofile resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/contentinspectionprofile? **view=summary**

Use this query-parameter to get the summary output of contentinspectionprofile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/contentinspectionprofile? **pagesize=#no;pageno=#no**

Use this query-parameter to get the contentinspectionprofile resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "contentinspectionprofile": [ {

"name":<String_value>,

"type":<String_value>,

"egressinterface":<String_value>,

"ingressinterface":<String_value>,

"egressvlan":<Integer_value>,

"ingressvlan":<Integer_value>,

"iptunnel":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/contentinspectionprofile/ name_value<String>
Query-parameters: attrs http:// <netscaler-ip-address> /nitro/v1/config/contentinspectionprofile/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/contentinspectionprofile/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of contentinspectionprofile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "contentinspectionprofile": [ {

"name":<String_value>,

"type":<String_value>,

"egressinterface":<String_value>,

"ingressinterface":<String_value>,

"egressvlan":<Integer_value>,

"ingressvlan":<Integer_value>,

"iptunnel":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/contentinspectionprofile? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "contentinspectionprofile": [ { "__count": "#no"} ] }
```

contentinspectionwasmprofile

Configuration for WASM profile resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of CI WASM profile. Minimum length = 1 Maximum length = 127

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
timeout	<Integer>	Read-write	Timeout (in milliseconds) for the connection with the CI WASM agent. Default value: 1000 Minimum value = 0 Maximum value = 86400000
timeoutaction	<String>	Read-write	Timeout action for the connection with the CI agent. Either the original request can be bypassed i.e. request/response is forwarded to the endpoint or the transaction is dropped/reset. Default value: DROP Possible values = BYPASS, DROP, RESET
maxbodylen	<Integer>	Read-write	Max data size (in KB) that will be sent to the CI Agent. Default is 16KB. Maximum value that can be configured is 32KB. Default value: 16 Minimum value = 0

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum value = 32
anomalousdatasize	<Integer>	Read-write	Transaction data size (in KB) greater than which a transaction is considered as anomalous. Default is 512KB. Default value: 512 Minimum value = 0 Maximum value = 512
anomalousttfbtime	<Integer>	Read-write	Transaction time (in milliseconds) above which a transaction is considered as anomalous. Default is 1 seconds. Default value: 1000 Minimum value = 0 Maximum value = 3600000
wasmmodule	<String>	Read-write	Name of the WASM Module. Minimum length = 1 Maximum length = 127
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/contentinspectionwasmprofile **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"contentinspectionwasmprofile":{

<b>"name":<String_value>,

</b>"timeout":<Integer_value>,

"timeoutaction":<String_value>,

"maxbodylen":<Integer_value>,

"anomalousdatasize":<Integer_value>,

"anomalousttfbtime":<Integer_value>,

<b>"wasmmodule":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/contentinspectionwasmprofile/name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/contentinspectionwasmprofile **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"contentinspectionwasmprofile":{

<b>"name":<String_value>,

</b>"timeout":<Integer_value>,

"timeoutaction":<String_value>,

"maxbodylen":<Integer_value>,

"anomalousdatasize":<Integer_value>,

"anomalousttfbtime":<Integer_value>,

"wasmmodule":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/contentinspectionwasmprofile? **action=unset**
HTTP Method: POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"contentinspectionwasmprofile":{

<b>"name":<String_value>,

</b>"timeout":true,

"timeoutaction":true,

"maxbodylen":true,

"anomalousdatasize":true,

"anomalousttfbtime":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/contentinspectionwasmprofile **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/contentinspectionwasmprofile? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/contentinspectionwasmprofile? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of contentinspectionwasmprofile resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/contentinspectionwasmprofile? **view=summary**

Use this query-parameter to get the summary output of contentinspectionwasmprofile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/contentinspectionwasmprofile? **pagesize=#no;pageno=#no**

Use this query-parameter to get the contentinspectionwasmprofile resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "contentinspectionwasmprofile": [ {

"name":<String_value>,

"timeout":<Integer_value>,

"timeoutaction":<String_value>,

"maxbodylen":<Integer_value>,

"anomalousdatasize":<Integer_value>,
```

```
"anomalousttfbtime":<Integer_value>,

"wasmmodule":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/contentinspectionwasmprofile/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/ contentinspectionwasmprofile/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/contentinspectionwasmprofile/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of contentinspectionwasmprofile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "contentinspectionwasmprofile": [ {

"name":<String_value>,

"timeout":<Integer_value>,

"timeoutaction":<String_value>,

"maxbodylen":<Integer_value>,

"anomalousdatasize":<Integer_value>,

"anomalousttfbtime":<Integer_value>,

"wasmmodule":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/contentinspectionwasmprofile? **count=yes**
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "contentinspectionwasmprofile": [ { "__count": "#no"} ] }
```

cr

Cache Redirection

Cache redirection configuration. The cache redirection feature can transparently redirect cacheable HTTP requests to a cache and send non-cacheable or dynamic HTTP requests to the origin server. A cache stores or caches frequently requested web content and serves such web content to a client on behalf of the origin servers, alleviating the load on the origin server farm.

NAME	DESCRIPTION
craction	Configuration for cache redirection action
crpolicy	Configuration for cache redirection policy
crpolicy_binding	Binding object showing the resources that can be bound to crpolicy
crpolicy_crvserver_binding	Binding object showing the crvserver that can be bound to crpolicy
crvserver	Configuration for CR virtual server
crvserver_analyticsprofile_binding	Binding object showing the analyticsprofile that can be bound to crvserver
crvserver_appflowpolicy_binding	Binding object showing the appflowpolicy that can be bound to crvserver
crvserver_appfwpolicy_binding	Binding object showing the appfwpolicy that can be bound to crvserver

NAME	DESCRIPTION
crvserver_appqoepolicy_binding	Binding object showing the appqoepolicy that can be bound to crvserver
crvserver_binding	Binding object showing the resources that can be bound to crvserver
crvserver_cachepolicy_binding	Binding object showing the cachepolicy that can be bound to crvserver
crvserver_cmppolicy_binding	Binding object showing the cmppolicy that can be bound to crvserver
crvserver_crpolicy_binding	Binding object showing the crpolicy that can be bound to crvserver
crvserver_cspolicy_binding	Binding object showing the cspolicy that can be bound to crvserver
crvserver_feopolicy_binding	Binding object showing the feopolicy that can be bound to crvserver
crvserver_icapolicy_binding	Binding object showing the icapolicy that can be bound to crvserver
crvserver_lbvserver_binding	Binding object showing the lbvserver that can be bound to crvserver
crvserver_policymap_binding	Binding object showing the policymap that can be bound to crvserver

NAME	DESCRIPTION
crvserver_responderpolicy_binding	Binding object showing the responderpolicy that can be bound to crvserver
crvserver_rewritepolicy_binding	Binding object showing the rewritepolicy that can be bound to crvserver
crvserver_spilloverpolicy_binding	Binding object showing the spilloverpolicy that can be bound to crvserver

craction

Configuration for cache redirection action resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the action for which to display detailed information. Minimum length = 1
crtype	<String>	Read-only	Type to decide where to redirect the requests if the cache redirection policy is hit. The valid options are as follows: *CACHE - Directs all the requests to the cache if cache redirection policy is hit.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			*ORIGIN - Directs all requests to the origin server if the cache redirection policy is hit. Possible values = origin, cache
builtin	<String[]>	Read-only	Flag to determine whether CRACTION is default or not. Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL
feature	<String>	Read-only	The feature to be checked while applying this config.
isdefault	<Boolean>	Read-only	A value of true is returned if it is a default cr action.
hits	<Integer>	Read-only	The number of times the action has been taken.
referencecount	<Integer>	Read-only	The number of references to the action.
undefhits	<Integer>	Read-only	The number of times the action resulted in UNDEF.
comment	<String>	Read-only	Comment. Any type of information about

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			this responder action.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/craction **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/craction? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/craction? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of craction resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/craction? **view=summary**

Use this query-parameter to get the summary output of craction resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/craction? **pagesize=#no;pageno=#no**

Use this query-parameter to get the craction resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "craction": [ {

"name":<String_value>,

"crtype":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"isdefault":<Boolean_value>,

"hits":<Integer_value>,

"referencecount":<Integer_value>,

"undefhits":<Integer_value>,

"comment":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/craction/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/craction/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/craction/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of craction resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "craction": [ {

"name":<String_value>,

"crtype":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"isdefault":<Boolean_value>,

"hits":<Integer_value>,

"referencecount":<Integer_value>,

"undefhits":<Integer_value>,

"comment":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/craction? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "craction": [ { "__count": "#no"} ] }
```

crpolicy

Configuration for cache redirection policy resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
policyname	<String>	Read-write	Name for the cache redirection policy. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at sign (@), equal sign (=), and hyphen (-) characters. Cannot

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			be changed after the policy is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my policy" or 'my policy'). Minimum length = 1
rule	<String>	Read-write	Expression, or name of a named expression, against which traffic is evaluated. The following requirements apply only to the Citrix ADC CLI: * If the expression includes one or more spaces, enclose the entire expression in double quotation marks. * If the expression itself includes double quotation

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			marks, escape the quotations by using the \ character. * Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks.
action	<String>	Read-write	Name of the built-in cache redirection action: CACHE/ ORIGIN.
logaction	<String>	Read-write	The log action associated with the cache redirection policy.
newname	<String>	Read-write	The new name of the content switching policy. Minimum length = 1
boundto	<String>	Read-only	Domain name.
vstype	<Integer>	Read-only	Virtual server type.
hits	<Integer>	Read-only	Total number of hits.
priority	<Integer>	Read-only	priority of bound policy.
activepolicy	<Boolean>	Read-only	Indicates whether policy is bound or not.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
labelname	<String>	Read-only	Name of the label invoked.
labeltype	<String>	Read-only	The invocation type. Possible values = reqvserver, resvserver, policylabel
builtin	<String[]>	Read-only	. Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL
feature	<String>	Read-only	The feature to be checked while applying this config.
isdefault	<Boolean>	Read-only	A value of true is returned if it is a default cr policy.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET

- COUNT
- RENAME

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/crpolicy **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"crpolicy":{

<b>"policyname":<String_value>,

</b><b>"rule":<String_value>,

</b>"action":<String_value>,

"logaction":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/crpolicy/ policyname_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/crpolicy **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"crpolicy":{

<b>"policyname":<String_value>,

</b>"rule":<String_value>,

"action":<String_value>,

"logaction":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/crpolicy? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"crpolicy":{

<b>"policyname":<String_value>,

</b>"logaction":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

RENAME

URL: http:// <netscaler-ip-address> /nitro/v1/config/crpolicy? **action=rename HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"crpolicy":{

<b>"policyname":<String_value>,

</b><b>"newname":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/crpolicy **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/crpolicy? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/crpolicy? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of crpolicy resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/crpolicy? **view=summary**

Use this query-parameter to get the summary output of crpolicy resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/crpolicy? **pagesize=#no;pageno=#no**

Use this query-parameter to get the crpolicy resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "crpolicy": [ {

"policyname":<String_value>,

"rule":<String_value>,

"boundto":<String_value>,

"action":<String_value>,

"vstype":<Integer_value>,

"hits":<Integer_value>,

"priority":<Integer_value>,

"activepolicy":<Boolean_value>,

"logaction":<String_value>,
```

```
"labelname":<String_value>,

"labeltype":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"isdefault":<Boolean_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/crpolicy/ policyname_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/crpolicy/ policyname_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/crpolicy/ policyname_value<String> ? **view=summary**

Use this query-parameter to get the summary output of crpolicy resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "crpolicy": [ {

"policyname":<String_value>,

"rule":<String_value>,

"boundto":<String_value>,

"action":<String_value>,

"vstype":<Integer_value>,

"hits":<Integer_value>,

"priority":<Integer_value>,

"activepolicy":<Boolean_value>,

"logaction":<String_value>,

"labelname":<String_value>,

"labeltype":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"isdefault":<Boolean_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/crpolicy? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "crpolicy": [ { "__count": "#no"} ] }
```

crpolicy_binding

Binding object which returns the resources bound to crpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
policyname	<String>	Read-write	Name of the cache redirection policy to display. If this parameter is omitted, details of all the policies are displayed. Minimum length = 1
crpolicy_crvserver_binding	<crpolicy_crvserver_binding[]>	Read-only	crvserver that can be bound to crpolicy.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/crpolicy_binding/ policyname_value<String>
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "crpolicy_binding": [ {

"policyname":<String_value>,

"crpolicy_crvserver_binding":<crpolicy_crvserver_binding[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/crpolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/crpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "crpolicy_binding": [ {

"policyname":<String_value>,

"crpolicy_crvserver_binding":<crpolicy_crvserver_binding[]_value>

}]}
```

crpolicy_crvserver_binding

Binding object showing the crvserver that can be bound to crpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
boundto	<String>	Read-write	Domain name.
policyname	<String>	Read-write	Name of the cache redirection policy to display. If this parameter is omitted, details of all the policies are displayed. Minimum length = 1
labelname	<String>	Read-only	Name of the label invoked.
gotopriorityexpression	<String>	Read-only	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
bindhits	<Integer>	Read-only	Total number of hits.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
hits	<Integer>	Read-only	Total number of hits.
priority	<Integer>	Read-only	priority of bound policy.
labeltype	<String>	Read-only	The invocation type. Possible values = reqvserver, resvserver, policylabel
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/crpolicy_crvserver_binding/ policyname_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ crpolicy_crvserver_binding/ policyname_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of crpolicy_crvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/crpolicy_crvserver_binding/ policyname_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the crpolicy_crvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "crpolicy_crvserver_binding": [ {

"boundto":<String_value>,
```

```
"policyname":<String_value>,

"labelname":<String_value>,

"gotopriorityexpression":<String_value>,

"bindhits":<Integer_value>,

"hits":<Integer_value>,

"priority":<Integer_value>,

"labeltype":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/crpolicy_crvserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/crpolicy_crvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "crpolicy_crvserver_binding": [ {

"boundto":<String_value>,

"policyname":<String_value>,

"labelname":<String_value>,

"gotopriorityexpression":<String_value>,

"bindhits":<Integer_value>,

"hits":<Integer_value>,

"priority":<Integer_value>,

"labeltype":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/crpolicy_crvserver_binding/ policyname_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"crpolicy_crvserver_binding": [ { "__count": "#no"} ] }
```

crvserver

Configuration for CR virtual server resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the cache redirection virtual server. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at sign (@), equal sign (=), and hyphen (-) characters. Can be changed after the cache redirection virtual server is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			marks (for example, "my server" or 'my server'). Minimum length = 1
td	<Integer>	Read-write	Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0. Minimum value = 0 Maximum value = 4094
servicetype	<String>	Read-write	Protocol (type of service) handled by the virtual server. Possible values = HTTP, SSL, NNTP, HDX
ipv46	<String>	Read-write	IPv4 or IPv6 address of the cache redirection virtual server. Usually a public IP address. Clients send connection requests to this IP address. Note: For a transparent cache redirection virtual

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			server, use an asterisk (*) to specify a wildcard virtual server address.
port	<Integer>	Read-write	Port number of the virtual server. Default value: 80 Minimum value = 1 Maximum value = 65534
ipset	<String>	Read-write	The list of IPv4/IPv6 addresses bound to ipset would form a part of listening service on the current cr vserver. Minimum length = 1
range	<Integer>	Read-write	Number of consecutive IP addresses, starting with the address specified by the IPAddress parameter, to include in a range of addresses assigned to this virtual server. Default value: 1 Minimum value = 1 Maximum value = 254

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
cachetype	<String>	Read-write	Mode of operation for the cache redirection virtual server. Available settings function as follows: * TRANSPARENT - Intercept all traffic flowing to the appliance and apply cache redirection policies to determine whether content should be served from the cache or from the origin server. * FORWARD - Resolve the hostname of the incoming request, by using a DNS server, and forward requests for non-cacheable content to the resolved origin servers. Cacheable requests are sent to the configured cache servers. * REVERSE - Configure reverse proxy caches for specific origin

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			servers. Incoming traffic directed to the reverse proxy can either be served from a cache server or be sent to the origin server with or without modification to the URL. The default value for cache type is TRANSPARENT if service is HTTP or SSL whereas the default cache type is FORWARD if the service is HDX. Possible values = TRANSPARENT, REVERSE, FORWARD
redirect	<String>	Read-write	Type of cache server to which to redirect HTTP requests. Available settings function as follows: * CACHE - Direct all requests to the cache. * POLICY - Apply the cache redirection policy to determine whether

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			the request should be directed to the cache or to the origin. * ORIGIN - Direct all requests to the origin server. Default value: POLICY Possible values = CACHE, POLICY, ORIGIN
onpolicymatch	<String>	Read-write	Redirect requests that match the policy to either the cache or the origin server, as specified. Note: For this option to work, you must set the cache redirection type to POLICY. Default value: ORIGIN Possible values = CACHE, ORIGIN
redirecturl	<String>	Read-write	URL of the server to which to redirect traffic if the cache redirection virtual server configured on the Citrix ADC

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			becomes unavailable. Minimum length = 1 Maximum length = 128
clttimeout	<Integer>	Read-write	Time-out value, in seconds, after which to terminate an idle client connection. Minimum value = 0 Maximum value = 31536000
precedence	<String>	Read-write	Type of policy (URL or RULE) that takes precedence on the cache redirection virtual server. Applies only to cache redirection virtual servers that have both URL and RULE based policies. If you specify URL, URL based policies are applied first, in the following order: 1. Domain and exact URL 2. Domain, prefix and suffix 3. Domain and suffix

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			4. Domain and prefix 5. Domain only 6. Exact URL 7. Prefix and suffix 8. Suffix only 9. Prefix only 10. Default If you specify RULE, the rule based policies are applied before URL based policies are applied. Default value: RULE Possible values = RULE, URL
arp	<String>	Read-write	Use ARP to determine the destination MAC address. Possible values = ON, OFF
ghost	<String>	Read-write	. Possible values = ON, OFF
map	<String>	Read-write	Obsolete.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ON, OFF
format	<String>	Read-write	. Possible values = ON, OFF
via	<String>	Read-write	Insert a via header in each HTTP request. In the case of a cache miss, the request is redirected from the cache server to the origin server. This header indicates whether the request is being sent from a cache server. Default value: ON Possible values = ON, OFF
cachevserver	<String>	Read-write	Name of the default cache virtual server to which to redirect requests (the default target of the cache redirection virtual server). Minimum length = 1
dnsvservername	<String>	Read-write	Name of the DNS virtual server that resolves domain names arriving at the forward proxy virtual server.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Note: This parameter applies only to forward proxy virtual servers, not reverse or transparent. Minimum length = 1
destinationvserver	<String>	Read-write	Destination virtual server for a transparent or forward proxy cache redirection virtual server. Minimum length = 1
domain	<String>	Read-write	Default domain for reverse proxies. Domains are configured to direct an incoming request from a specified source domain to a specified target domain. There can be several configured pairs of source and target domains. You can select one pair to be the default. If the host header or URL of an incoming request does not include a source domain, this option sends the request to the specified target domain.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum length = 1
sopersistencetimeout	<Integer>	Read-write	Time-out, in minutes, for spillover persistence. Minimum value = 2 Maximum value = 24
sothreshold	<Integer>	Read-write	For CONNECTION (or) DYNAMICCONNECTION spillover, the number of connections above which the virtual server enters spillover mode. For BANDWIDTH spillover, the amount of incoming and outgoing traffic (in Kbps) before spillover. For HEALTH spillover, the percentage of active services (by weight) below which spillover occurs. Minimum value = 1
reuse	<String>	Read-write	Reuse TCP connections to the origin server across client connections. Do not set this parameter unless the Service Type parameter is set to HTTP. If you set this

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			parameter to OFF, the possible settings of the Redirect parameter function as follows: * CACHE - TCP connections to the cache servers are not reused. * ORIGIN - TCP connections to the origin servers are not reused. * POLICY - TCP connections to the origin servers are not reused. If you set the Reuse parameter to ON, connections to origin servers and connections to cache servers are reused. Default value: ON Possible values = ON, OFF
state	<String>	Read-write	Initial state of the cache redirection virtual server. Default value: ENABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ENABLED, DISABLED
downstateflush	<String>	Read-write	Perform delayed cleanup of connections to this virtual server. Default value: ENABLED Possible values = ENABLED, DISABLED
backupvserver	<String>	Read-write	Name of the backup virtual server to which traffic is forwarded if the active server becomes unavailable. Minimum length = 1
disableprimaryondown	<String>	Read-write	Continue sending traffic to a backup virtual server even after the primary virtual server comes UP from the DOWN state. Default value: DISABLED Possible values = ENABLED, DISABLED
l2conn	<String>	Read-write	Use L2 parameters, such as MAC, VLAN,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			and channel to identify a connection. Possible values = ON, OFF
backendssl	<String>	Read-write	Decides whether the backend connection made by Citrix ADC to the origin server will be HTTP or SSL. Applicable only for SSL type CR Forward proxy vserver. Default value: DISABLED Possible values = ENABLED, DISABLED
listenpolicy	<String>	Read-write	String specifying the listen policy for the cache redirection virtual server. Can be either an in-line expression or the name of a named expression. Default value: "NONE"
listenpriority	<Integer>	Read-write	Priority of the listen policy specified by the Listen Policy parameter. The lower the number, higher the priority. Default value: 101

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum value = 0 Maximum value = 100
tcpprofilename	<String>	Read-write	Name of the profile containing TCP configuration information for the cache redirection virtual server. Minimum length = 1 Maximum length = 127
httpprofilename	<String>	Read-write	Name of the profile containing HTTP configuration information for cache redirection virtual server. Minimum length = 1 Maximum length = 127
comment	<String>	Read-write	Comments associated with this virtual server. Maximum length = 256
srcipexpr	<String>	Read-write	Expression used to extract the source IP addresses from the requests originating from the cache. Can be either an in-line expression or the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			name of a named expression. Minimum length = 1 Maximum length = 1500
originusip	<String>	Read-write	Use the client's IP address as the source IP address in requests sent to the origin server. Note: You can enable this parameter to implement fully transparent CR deployment. Possible values = ON, OFF
useportrange	<String>	Read-write	Use a port number from the port range (set by using the set ns param command, or in the Create Virtual Server (Cache Redirection) dialog box) as the source port in the requests sent to the origin server. Default value: OFF Possible values = ON, OFF
appflowlog	<String>	Read-write	Enable logging of AppFlow information.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: ENABLED Possible values = ENABLED, DISABLED
netprofile	<String>	Read-write	Name of the network profile containing network configurations for the cache redirection virtual server. Minimum length = 1 Maximum length = 127
icmpvsrresponse	<String>	Read-write	Criterion for responding to PING requests sent to this virtual server. If ACTIVE, respond only if the virtual server is available. If PASSIVE, respond even if the virtual server is not available. Default value: PASSIVE Possible values = PASSIVE, ACTIVE
rhistate	<String>	Read-write	A host route is injected according to the setting on the virtual servers

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			* If set to PASSIVE on all the virtual servers that share the IP address, the appliance always injects the hostroute. * If set to ACTIVE on all the virtual servers that share the IP address, the appliance injects even if one virtual server is UP. * If set to ACTIVE on some virtual servers and PASSIVE on the others, the appliance, injects even if one virtual server set to ACTIVE is UP. Default value: PASSIVE Possible values = PASSIVE, ACTIVE
useoriginipportforcache	<String>	Read-write	Use origin ip/port while forwarding request to the cache. Change the destination IP, destination port of the request came to

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			CR vserver to Origin IP and Origin Port and forward it to Cache. Default value: NO Possible values = YES, NO
tcpprobeport	<Integer>	Read-write	Port number for external TCP probe. NetScaler provides support for external TCP health check of the vserver status over the selected port. This option is only supported for vservers assigned with an IPAddress or ipset. Minimum value = 1 Range 1 - 65535 * in CLI is represented as 65535 in NITRO API
probeprotocol	<String>	Read-write	Citrix ADC provides support for external health check of the vserver status. Select HTTP or TCP probes for healthcheck. Possible values = TCP, HTTP

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
probesuccessresponsecode	<String>	Read-write	HTTP code to return in SUCCESS case. Default value: "200 OK" Minimum length = 1 Maximum length = 64
probeport	<Integer>	Read-write	Citrix ADC provides support for external health check of the vserver status. Select port for HTTP/TCP monitring. Default value: 0 Range 1 - 65535 * in CLI is represented as 65535 in NITRO API
disallowserviceaccess	<String>	Read-write	This is effective when a FORWARD type cr vserver is added. By default, this parameter is DISABLED. When it is ENABLED, backend services cannot be accessed through a FORWARD type cr vserver. Default value: DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ENABLED, DISABLED
wasmmodule	<String>	Read-write	Name of the WASM module to assign to this virtual server.
newname	<String>	Read-write	New name for the cache redirection virtual server. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at sign (@), equal sign (=), and hyphen (-) characters. If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my name" or 'my name'). Minimum length = 1
ip	<String>	Read-only	.
value	<String>	Read-only	The ssl card status for the transparent ssl cr vserver. Possible values = Certkey/ Certkeybundle/Vault

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			not bound/Cert-store not usable, SSL feature disabled
ngname	<String>	Read-only	Nodegroup devno to which this crvserver belongs to.
type	<String>	Read-only	Virtual server type. Possible values = CONTENT, ADDRESS
curstate	<String>	Read-only	The state of the cr vserver. Possible values = UP, DOWN, UNKNOWN, BUSY, OUT OF SERVICE, GOING OUT OF SERVICE, DOWN WHEN GOING OUT OF SERVICE, NS_EMPTY_STR, Unknown, DISABLED
status	<Integer>	Read-only	Status.
authentication	<String>	Read-only	Authentication. Possible values = ON, OFF
homepage	<String>	Read-only	Home page.
rule	<String>	Read-only	Rule.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
policyname	<String>	Read-only	Policies bound to this vserver.
pipolicyhits	<Integer>	Read-only	Number of hits.
servicename	<String>	Read-only	Service name.
weight	<Integer>	Read-only	Weight for this service.
targetvserver	<String>	Read-only	The CSW target server names.
priority	<Integer>	Read-only	The priority for the policy.
somethod	<String>	Read-only	The spillover factor. When the main virtual server reaches this spillover threshold, it will give further traffic to the backupvserver. Possible values = CONNECTION, DYNAMICCONNECTION, BANDWIDTH, HEALTH, LLMQUOTA, NONE
sopersistence	<String>	Read-only	The state of spillover persistence. Possible values = ENABLED, DISABLED
lbvserver	<String>	Read-only	The Default target server name.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum length = 1
bindpoint	<String>	Read-only	The bindpoint to which the policy is bound. Possible values = REQUEST, RESPONSE, ICA_REQUEST
invoke	<Boolean>	Read-only	Invoke flag.
labeltype	<String>	Read-only	The invocation type. Possible values = reqvserver, resvserver, policylabel
labelname	<String>	Read-only	Name of the label invoked.
gotopriorityexpression	<String>	Read-only	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
nodefaultbindings	<String>	Read-only	to determine if the configuration will have default ssl CIPHER and ECC curve bindings. Default value: NO Possible values = YES, NO
_nextgenapiresource	<String>	Read-only	.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- ENABLE
- DISABLE
- GET (ALL)
- GET
- COUNT
- RENAME

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/crvserver **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"crvserver":{

<b>"name":<String_value>,

</b>"td":<Integer_value>,

<b>"servicetype":<String_value>,

</b>"ipv46":<String_value>,

"port":<Integer_value>,

"ipset":<String_value>,

"range":<Integer_value>,

"cachetype":<String_value>,

"redirect":<String_value>,

"onpolicymatch":<String_value>,

"redirecturl":<String_value>,

"clttimeout":<Integer_value>,
```

```
"precedence":<String_value>,

"arp":<String_value>,

"ghost":<String_value>,

"map":<String_value>,

"format":<String_value>,

"via":<String_value>,

"cachevserver":<String_value>,

"dnsvservername":<String_value>,

"destinationvserver":<String_value>,

"domain":<String_value>,

"sopersistencetimeout":<Integer_value>,

"sothreshold":<Integer_value>,

"reuse":<String_value>,

"state":<String_value>,

"downstateflush":<String_value>,

"backupvserver":<String_value>,

"disableprimaryondown":<String_value>,

"l2conn":<String_value>,

"backendssl":<String_value>,

"listenpolicy":<String_value>,

"listenpriority":<Integer_value>,

"tcpprofilename":<String_value>,
```

```
"httpprofilename":<String_value>,

"comment":<String_value>,

"srcipexpr":<String_value>,

"originusip":<String_value>,

"useportrange":<String_value>,

"appflowlog":<String_value>,

"netprofile":<String_value>,

"icmpvsrresponse":<String_value>,

"rhistate":<String_value>,

"useoriginipportforcache":<String_value>,

"tcpprobeport":<Integer_value>,

"probeprotocol":<String_value>,

"probesuccessresponsecode":<String_value>,

"probeport":<Integer_value>,

"disallowserviceaccess":<String_value>,

"wasmmodule":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/crvserver/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/crvserver **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"crvserver":{

<b>"name":<String_value>,

</b>"ipv46":<String_value>,

"ipset":<String_value>,

"redirect":<String_value>,

"onpolicymatch":<String_value>,

"precedence":<String_value>,

"arp":<String_value>,

"via":<String_value>,

"cachevserver":<String_value>,
```

```
"dnsvservername":<String_value>,

"destinationvserver":<String_value>,

"domain":<String_value>,

"reuse":<String_value>,

"backupvserver":<String_value>,

"disableprimaryondown":<String_value>,

"redirecturl":<String_value>,

"clttimeout":<Integer_value>,

"downstateflush":<String_value>,

"l2conn":<String_value>,

"backendssl":<String_value>,

"listenpolicy":<String_value>,

"listenpriority":<Integer_value>,

"tcpprofilename":<String_value>,

"httpprofilename":<String_value>,

"netprofile":<String_value>,

"comment":<String_value>,

"srcipexpr":<String_value>,

"originusip":<String_value>,

"useportrange":<String_value>,

"appflowlog":<String_value>,

"icmpvsrresponse":<String_value>,
```

```
"rhistate":<String_value>,

"useoriginipportforcache":<String_value>,

"tcpprobeport":<Integer_value>,

"probeprotocol":<String_value>,

"probesuccessresponsecode":<String_value>,

"probeport":<Integer_value>,

"disallowserviceaccess":<String_value>,

"wasmmodule":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/crvserver? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"crvserver":{

<b>"name":<String_value>,

</b>"cachevserver":true,
```

```
"dnsvservername":true,
"destinationvserver":true,
"domain":true,
"backupvserver":true,
"clttimeout":true,
"redirecturl":true,
"l2conn":true,
"backendssl":true,
"originusip":true,
"useportrange":true,
"srcipexpr":true,
"tcpprofilename":true,
"httpprofilename":true,
"appflowlog":true,
"netprofile":true,
"icmpvsrresponse":true,
"tcpprobeport":true,
"probeprotocol":true,
"wasmmodule":true,
"ipset":true,
"redirect":true,
"onpolicymatch":true,
```

```
"precedence":true,

"arp":true,

"via":true,

"reuse":true,

"disableprimaryondown":true,

"downstateflush":true,

"listenpolicy":true,

"listenpriority":true,

"comment":true,

"rhistate":true,

"useoriginipportforcache":true,

"probesuccessresponsecode":true,

"disallowserviceaccess":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

ENABLE

URL: http:// <netscaler-ip-address> /nitro/v1/config/crvserver? **action=enable HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"crvserver":{

<b>"name":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DISABLE

URL: http:// <netscaler-ip-address> /nitro/v1/config/crvserver? **action=disable HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"crvserver":{

<b>"name":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

RENAME

URL: http:// <netscaler-ip-address> /nitro/v1/config/crvserver? **action=rename HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"crvserver":{

<b>"name":<String_value>,

</b><b>"newname":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/crvserver **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/crvserver? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/crvserver? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of crvserver resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/crvserver? **view=summary**

Use this query-parameter to get the summary output of crvserver resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/crvserver? **pagesize=#no;pageno=#no**

Use this query-parameter to get the crvserver resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "crvserver": [ {

"name":<String_value>,

"ip":<String_value>,

"td":<Integer_value>,

"ipv46":<String_value>,

"value":<String_value>,

"port":<Integer_value>,

"range":<Integer_value>,

"servicetype":<String_value>,

"ngname":<String_value>,

"type":<String_value>,

"curstate":<String_value>,

"status":<Integer_value>,
```

```
"cachetype":<String_value>,

"redirect":<String_value>,

"onpolicymatch":<String_value>,

"precedence":<String_value>,

"redirecturl":<String_value>,

"authentication":<String_value>,

"homepage":<String_value>,

"dnsvservername":<String_value>,

"domain":<String_value>,

"rule":<String_value>,

"policyname":<String_value>,

"pipolicyhits":<Integer_value>,

"servicename":<String_value>,

"weight":<Integer_value>,

"cachevserver":<String_value>,

"targetvserver":<String_value>,

"backupvserver":<String_value>,

"priority":<Integer_value>,

"clttimeout":<Integer_value>,

"somethod":<String_value>,

"sopersistence":<String_value>,

"sopersistencetimeout":<Integer_value>,
```

```
"sothreshold":<Integer_value>,

"reuse":<String_value>,

"arp":<String_value>,

"destinationvserver":<String_value>,

"via":<String_value>,

"downstateflush":<String_value>,

"disableprimaryondown":<String_value>,

"l2conn":<String_value>,

"backendssl":<String_value>,

"comment":<String_value>,

"listenpolicy":<String_value>,

"listenpriority":<Integer_value>,

"tcpprofilename":<String_value>,

"httpprofilename":<String_value>,

"srcipexpr":<String_value>,

"originusip":<String_value>,

"useportrange":<String_value>,

"appflowlog":<String_value>,

"netprofile":<String_value>,

"icmpvsrresponse":<String_value>,

"rhistate":<String_value>,

"lbvserver":<String_value>,
```

```
"bindpoint":<String_value>,

"invoke":<Boolean_value>,

"labeltype":<String_value>,

"labelname":<String_value>,

"gotopriorityexpression":<String_value>,

"ipset":<String_value>,

"nodefaultbindings":<String_value>,

"useoriginipportforcache":<String_value>,

"tcpprobeport":<Integer_value>,

"probeprotocol":<String_value>,

"probeport":<Integer_value>,

"probesuccessresponsecode":<String_value>,

"disallowserviceaccess":<String_value>,

"wasmmodule":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/crvserver/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/crvserver/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/crvserver/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of crvserver resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "crvserver": [ {

"name":<String_value>,

"ip":<String_value>,

"td":<Integer_value>,

"ipv46":<String_value>,

"value":<String_value>,

"port":<Integer_value>,

"range":<Integer_value>,

"servicetype":<String_value>,

"ngname":<String_value>,
```

```
"type":<String_value>,

"curstate":<String_value>,

"status":<Integer_value>,

"cachetype":<String_value>,

"redirect":<String_value>,

"onpolicymatch":<String_value>,

"precedence":<String_value>,

"redirecturl":<String_value>,

"authentication":<String_value>,

"homepage":<String_value>,

"dnsvservername":<String_value>,

"domain":<String_value>,

"rule":<String_value>,

"policyname":<String_value>,

"pipolicyhits":<Integer_value>,

"servicename":<String_value>,

"weight":<Integer_value>,

"cachevserver":<String_value>,

"targetvserver":<String_value>,

"backupvserver":<String_value>,

"priority":<Integer_value>,

"clttimeout":<Integer_value>,
```

```
"somethod":<String_value>,

"sopersistence":<String_value>,

"sopersistencetimeout":<Integer_value>,

"sothreshold":<Integer_value>,

"reuse":<String_value>,

"arp":<String_value>,

"destinationvserver":<String_value>,

"via":<String_value>,

"downstateflush":<String_value>,

"disableprimaryondown":<String_value>,

"l2conn":<String_value>,

"backendssl":<String_value>,

"comment":<String_value>,

"listenpolicy":<String_value>,

"listenpriority":<Integer_value>,

"tcpprofilename":<String_value>,

"httpprofilename":<String_value>,

"srcipexpr":<String_value>,

"originusip":<String_value>,

"useportrange":<String_value>,

"appflowlog":<String_value>,

"netprofile":<String_value>,
```

```
"icmpvsrresponse":<String_value>,

"rhistate":<String_value>,

"lbvserver":<String_value>,

"bindpoint":<String_value>,

"invoke":<Boolean_value>,

"labeltype":<String_value>,

"labelname":<String_value>,

"gotopriorityexpression":<String_value>,

"ipset":<String_value>,

"nodefaultbindings":<String_value>,

"useoriginipportforcache":<String_value>,

"tcpprobeport":<Integer_value>,

"probeprotocol":<String_value>,

"probeport":<Integer_value>,

"probesuccessresponsecode":<String_value>,

"disallowserviceaccess":<String_value>,

"wasmmodule":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/crvserver? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "crvserver": [ { "__count": "#no"} ] }
```

crvserver_analyticsprofile_binding

Binding object showing the analyticsprofile that can be bound to crvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the cache redirection virtual server to which to bind the cache redirection policy. Minimum length = 1
analyticsprofile	<String>	Read-write	Name of the analytics profile bound to the CR vserver.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/crvserver_analyticsprofile_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"crvserver_analyticsprofile_binding":{

<b>"name":<String_value>,

</b>"analyticsprofile":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/crvserver_analyticsprofile_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ crvserver_analyticsprofile_binding/ name_value<String> ? **args=analyticsprofile: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/crvserver_analyticsprofile_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/

crvserver_analyticsprofile_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of crvserver_analyticsprofile_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/crvserver_analyticsprofile_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the crvserver_analyticsprofile_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "crvserver_analyticsprofile_binding": [ {

"name":<String_value>,

"analyticsprofile":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/crvserver_analyticsprofile_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/crvserver_analyticsprofile_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "crvserver_analyticsprofile_binding": [ {

"name":<String_value>,

"analyticsprofile":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/crvserver_analyticsprofile_binding/name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"crvserver_analyticsprofile_binding": [ { "__count": "#no"} ] }
```

crvserver_appflowpolicy_binding

Binding object showing the appflowpolicy that can be bound to crvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the cache redirection virtual server to which to bind the cache redirection policy. Minimum length = 1
labeltype	<String>	Read-write	The invocation type. Possible values = reqvserver, resvserver, policylabel
priority	<Integer>	Read-write	The priority for the policy.
bindpoint	<String>	Read-write	For a rewrite policy, the bind point to which to bind the policy. Note: This parameter applies

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			only to rewrite policies, because content switching policies are evaluated only at request time. Possible values = REQUEST, RESPONSE, ICA_REQUEST
labelname	<String>	Read-write	Name of the label invoked.
targetvserver	<String>	Read-write	Name of the virtual server to which content is forwarded. Applicable only if the policy is a map policy and the cache redirection virtual server is of type REVERSE. Minimum length = 1
gotopriorityexpression	<String>	Read-write	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
invoke	<Boolean>	Read-write	Invoke flag.
policyname	<String>	Read-write	Policies bound to this vserver.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/crvserver_appflowpolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"crvserver_appflowpolicy_binding":{

<b>"name":<String_value>,

</b>"policyname":<String_value>,

"targetvserver":<String_value>,

"priority":<Integer_value>,

"gotopriorityexpression":<String_value>,

"bindpoint":<String_value>,

"invoke":<Boolean_value>,

"labeltype":<String_value>,

"labelname":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/crvserver_appflowpolicy_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ crvserver_appflowpolicy_binding/ name_value<String> ? **args=policyname: <String_value> ,bindpoint: <String_value> ,priority: <Integer_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/crvserver_appflowpolicy_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ crvserver_appflowpolicy_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of crvserver_appflowpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/crvserver_appflowpolicy_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the crvserver_appflowpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "crvserver_appflowpolicy_binding": [ {

"name":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"bindpoint":<String_value>,

"labelname":<String_value>,

"targetvserver":<String_value>,

"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>,

"policyname":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/crvserver_appflowpolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/crvserver_appflowpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "crvserver_appflowpolicy_binding": [ {

"name":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"bindpoint":<String_value>,

"labelname":<String_value>,

"targetvserver":<String_value>,

"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>,

"policyname":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/crvserver_appflowpolicy_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"crvserver_appflowpolicy_binding": [ { "__count": "#no"} ] }
```

crvserver_appfwpolicy_binding

Binding object showing the appfwpolicy that can be bound to crvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
targetvserver	<String>	Read-write	Name of the virtual server to which content is forwarded. Applicable only if the policy is a map policy and the cache redirection virtual server is of type REVERSE. Minimum length = 1
policyname	<String>	Read-write	Policies bound to this vserver.
invoke	<Boolean>	Read-write	Invoke flag.
gotopriorityexpression	<String>	Read-write	Expression specifying the priority of the next policy which will get evaluated if the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			current policy rule evaluates to TRUE.
name	<String>	Read-write	Name of the cache redirection virtual server to which to bind the cache redirection policy. Minimum length = 1
priority	<Integer>	Read-write	The priority for the policy.
labeltype	<String>	Read-write	The invocation type. Possible values = reqvserver, resvserver, policylabel
bindpoint	<String>	Read-write	The bindpoint to which the policy is bound. Possible values = REQUEST, RESPONSE, ICA_REQUEST
labelname	<String>	Read-write	Name of the label invoked.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET

- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/crvserver_appfwpolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"crvserver_appfwpolicy_binding":{

<b>"name":<String_value>,

</b>"policyname":<String_value>,

"targetvserver":<String_value>,

"priority":<Integer_value>,

"gotopriorityexpression":<String_value>,

"bindpoint":<String_value>,

"invoke":<Boolean_value>,

"labeltype":<String_value>,

"labelname":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/crvserver_appfwpolicy_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ crvserver_appfwpolicy_binding/ name_value<String> ? **args=policyname: <String_value> ,bindpoint: <String_value> ,priority: <Integer_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/crvserver_appfwpolicy_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ crvserver_appfwpolicy_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of crvserver_appfwpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/crvserver_appfwpolicy_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the crvserver_appfwpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "crvserver_appfwpolicy_binding": [ {

"targetvserver":<String_value>,

"policyname":<String_value>,

"invoke":<Boolean_value>,
```

```
"gotopriorityexpression":<String_value>,

"name":<String_value>,

"priority":<Integer_value>,

"labeltype":<String_value>,

"bindpoint":<String_value>,

"labelname":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/crvserver_appfwpolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/crvserver_appfwpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "crvserver_appfwpolicy_binding": [ {

"targetvserver":<String_value>,

"policyname":<String_value>,

"invoke":<Boolean_value>,

"gotopriorityexpression":<String_value>,

"name":<String_value>,

"priority":<Integer_value>,

"labeltype":<String_value>,

"bindpoint":<String_value>,

"labelname":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/crvserver_appfwpolicy_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"crvserver_appfwpolicy_binding": [ { "__count": "#no"} ] }
```

crvserver_appqoepolicy_binding

Binding object showing the appqoepolicy that can be bound to crvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
labeltype	<String>	Read-write	The invocation type. Possible values = reqvserver, resvserver, policylabel
priority	<Integer>	Read-write	The priority for the policy.
bindpoint	<String>	Read-write	The bindpoint to which the policy is bound. Possible values = REQUEST, RESPONSE, ICA_REQUEST
name	<String>	Read-write	Name of the cache redirection virtual server to which to bind the cache redirection policy. Minimum length = 1
labelname	<String>	Read-write	Name of the label invoked.
targetvserver	<String>	Read-write	Name of the virtual server to which

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			content is forwarded. Applicable only if the policy is a map policy and the cache redirection virtual server is of type REVERSE. Minimum length = 1
policyname	<String>	Read-write	Policies bound to this vserver.
gotopriorityexpression	<String>	Read-write	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
invoke	<Boolean>	Read-write	Invoke flag.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/crvserver_appqoepolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"crvserver_appqoepolicy_binding":{

<b>"name":<String_value>,

</b>"policyname":<String_value>,

"targetvserver":<String_value>,
```

```
"priority":<Integer_value>,

"gotopriorityexpression":<String_value>,

"bindpoint":<String_value>,

"invoke":<Boolean_value>,

"labeltype":<String_value>,

"labelname":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/crvserver_appqoepolicy_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ crvserver_appqoepolicy_binding/ name_value<String> ? **args=policyname: <String_value> ,bindpoint: <String_value> ,priority: <Integer_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/crvserver_appqoepolicy_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/

crvserver_appqoepolicy_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of crvserver_appqoepolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/crvserver_appqoepolicy_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the crvserver_appqoepolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "crvserver_appqoepolicy_binding": [ {

"labeltype":<String_value>,

"priority":<Integer_value>,

"bindpoint":<String_value>,

"name":<String_value>,

"labelname":<String_value>,

"targetvserver":<String_value>,
```

```
"policyname":<String_value>,

"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/crvserver_appqoepolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/crvserver_appqoepolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "crvserver_appqoepolicy_binding": [ {

"labeltype":<String_value>,

"priority":<Integer_value>,
```

```
"bindpoint":<String_value>,

"name":<String_value>,

"labelname":<String_value>,

"targetvserver":<String_value>,

"policyname":<String_value>,

"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/crvserver_appqoepolicy_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"crvserver_appqoepolicy_binding": [ { "__count": "#no"} ] }
```

crvserver_binding

Binding object which returns the resources bound to crvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of a cache redirection virtual server about which to display detailed information. Minimum length = 1
crvserver_lbvserver_binding	<crvserver_lbvserver_binding[]>	Read-only	lbvserver that can be bound to crvserver.
crvserver_cmppolicy_binding	<crvserver_cmppolicy_binding[]>	Read-only	cmppolicy that can be bound to crvserver.
crvserver_appfwpolicy_binding	<crvserver_appfwpolicy_binding[]>	Read-only	appfwpolicy that can be bound to crvserver.
crvserver_cspolicy_binding	<crvserver_cspolicy_binding[]>	Read-only	cspolicy that can be bound to crvserver.
crvserver_policymap_binding	<crvserver_policymap_binding[]>	Read-only	policymap that can be bound to crvserver.
crvserver_cachepolicy_binding	<crvserver_cachepolicy_binding[]>	Read-only	cachepolicy that can be bound to crvserver.
crvserver_feopolicy_binding	<crvserver_feopolicy_binding[]>	Read-only	feopolicy that can be bound to crvserver.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
crvserver_spilloverpolicy_binding	<crvserver_spilloverpolicy_binding[]>	Read-only	spilloverpolicy that can be bound to crvserver.
crvserver_rewritepolicy_binding	<crvserver_rewritepolicy_binding[]>	Read-only	rewritepolicy that can be bound to crvserver.
crvserver_appflowpolicy_binding	<crvserver_appflowpolicy_binding[]>	Read-only	appflowpolicy that can be bound to crvserver.
crvserver_analyticsprofile_binding	<crvserver_analyticsprofile_binding[]>	Read-only	analyticsprofile that can be bound to crvserver.
crvserver_appqoepolicy_binding	<crvserver_appqoepolicy_binding[]>	Read-only	appqoepolicy that can be bound to crvserver.
crvserver_icapolicy_binding	<crvserver_icapolicy_binding[]>	Read-only	icapolicy that can be bound to crvserver.
crvserver_responderpolicy_binding	<crvserver_responderpolicy_binding[]>	Read-only	responderpolicy that can be bound to crvserver.
crvserver_crpolicy_binding	<crvserver_crpolicy_binding[]>	Read-only	crpolicy that can be bound to crvserver.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/crvserver_binding/ name_value<String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "crvserver_binding": [ {

"name":<String_value>,

"crvserver_feopolicy_binding":<crvserver_feopolicy_binding[]_value>,

"crvserver_policymap_binding":<crvserver_policymap_binding[]_value>,

"crvserver_crpolicy_binding":<crvserver_crpolicy_binding[]_value>,

"crvserver_cmppolicy_binding":<crvserver_cmppolicy_binding[]_value>,

"crvserver_analyticsprofile_binding":<crvserver_analyticsprofile_binding[]
_value>,

"crvserver_lbvserver_binding":<crvserver_lbvserver_binding[]_value>,

"crvserver_appflowpolicy_binding":<crvserver_appflowpolicy_binding[]_value
>,

"crvserver_spilloverpolicy_binding":<crvserver_spilloverpolicy_binding[]_v
alue>,

"crvserver_appfwpolicy_binding":<crvserver_appfwpolicy_binding[]_value>,

"crvserver_icapolicy_binding":<crvserver_icapolicy_binding[]_value>,

"crvserver_cspolicy_binding":<crvserver_cspolicy_binding[]_value>,

"crvserver_cachepolicy_binding":<crvserver_cachepolicy_binding[]_value>,

"crvserver_rewritepolicy_binding":<crvserver_rewritepolicy_binding[]_value
>,

"crvserver_appqoepolicy_binding":<crvserver_appqoepolicy_binding[]_value>,

"crvserver_responderpolicy_binding":<crvserver_responderpolicy_binding[]_v
alue>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/crvserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/crvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "crvserver_binding": [ {

"name":<String_value>,

"crvserver_feopolicy_binding":<crvserver_feopolicy_binding[]_value>,

"crvserver_policymap_binding":<crvserver_policymap_binding[]_value>,

"crvserver_crpolicy_binding":<crvserver_crpolicy_binding[]_value>,

"crvserver_cmppolicy_binding":<crvserver_cmppolicy_binding[]_value>,

"crvserver_analyticsprofile_binding":<crvserver_analyticsprofile_binding[]
_value>,
```

```
"crvserver_lbvserver_binding":<crvserver_lbvserver_binding[]_value>,

"crvserver_appflowpolicy_binding":<crvserver_appflowpolicy_binding[]_value
>,

"crvserver_spilloverpolicy_binding":<crvserver_spilloverpolicy_binding[]_v
alue>,

"crvserver_appfwpolicy_binding":<crvserver_appfwpolicy_binding[]_value>,

"crvserver_icapolicy_binding":<crvserver_icapolicy_binding[]_value>,

"crvserver_cspolicy_binding":<crvserver_cspolicy_binding[]_value>,

"crvserver_cachepolicy_binding":<crvserver_cachepolicy_binding[]_value>,

"crvserver_rewritepolicy_binding":<crvserver_rewritepolicy_binding[]_value
>,

"crvserver_appqoepolicy_binding":<crvserver_appqoepolicy_binding[]_value>,

"crvserver_responderpolicy_binding":<crvserver_responderpolicy_binding[]_v
alue>

}]}
```

crvserver_cachepolicy_binding

Binding object showing the cachepolicy that can be bound to crvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
targetvserver	<String>	Read-write	Name of the virtual server to which content is forwarded. Applicable only if the policy is a map policy and the cache

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			redirection virtual server is of type REVERSE. Minimum length = 1
gotopriorityexpression	<String>	Read-write	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
invoke	<Boolean>	Read-write	Invoke flag.
policyname	<String>	Read-write	Policies bound to this vserver.
bindpoint	<String>	Read-write	The bindpoint to which the policy is bound. Possible values = REQUEST, RESPONSE, ICA_REQUEST
labeltype	<String>	Read-write	The invocation type. Possible values = reqvserver, resvserver, policylabel
priority	<Integer>	Read-write	The priority for the policy.
name	<String>	Read-write	Name of the cache redirection virtual server to which to bind the cache redirection policy.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum length = 1
labelname	<String>	Read-write	Name of the label invoked.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/crvserver_cachepolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"crvserver_cachepolicy_binding":{

<b>"name":<String_value>,

</b>"policyname":<String_value>,

"targetvserver":<String_value>,

"priority":<Integer_value>,

"gotopriorityexpression":<String_value>,

"bindpoint":<String_value>,

"invoke":<Boolean_value>,

"labeltype":<String_value>,

"labelname":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/crvserver_cachepolicy_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ crvserver_cachepolicy_binding/ name_value<String> ? **args=policyname: <String_value> ,bindpoint: <String_value> ,priority: <Integer_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/crvserver_cachepolicy_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ crvserver_cachepolicy_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of crvserver_cachepolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/crvserver_cachepolicy_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the crvserver_cachepolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "crvserver_cachepolicy_binding": [ {

"targetvserver":<String_value>,

"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>,

"policyname":<String_value>,

"bindpoint":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"name":<String_value>,

"labelname":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/crvserver_cachepolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ crvserver_cachepolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "crvserver_cachepolicy_binding": [ {

"targetvserver":<String_value>,

"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>,

"policyname":<String_value>,

"bindpoint":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"name":<String_value>,

"labelname":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/crvserver_cachepolicy_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"crvserver_cachepolicy_binding": [ { "__count": "#no"} ] }
```

crvserver_cmppolicy_binding

Binding object showing the cmppolicy that can be bound to crvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
labelname	<String>	Read-write	Name of the label invoked.
name	<String>	Read-write	Name of the cache redirection virtual server to which to bind the cache redirection policy. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
bindpoint	<String>	Read-write	The bindpoint to which the policy is bound. Possible values = REQUEST, RESPONSE, ICA_REQUEST
priority	<Integer>	Read-write	The priority for the policy.
labeltype	<String>	Read-write	The invocation type. Possible values = reqvserver, resvserver, policylabel
policyname	<String>	Read-write	Policies bound to this vserver.
invoke	<Boolean>	Read-write	Invoke flag.
gotopriorityexpression	<String>	Read-write	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
targetvserver	<String>	Read-write	Name of the virtual server to which content is forwarded. Applicable only if the policy is a map policy and the cache redirection virtual server is of type REVERSE.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum length = 1
inherited	<String>	Read-only	On State describes that policy bound is inherited from global binding. Possible values = ON, OFF
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/crvserver_cmppolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"crvserver_cmppolicy_binding":{

<b>"name":<String_value>,

</b>"policyname":<String_value>,

"targetvserver":<String_value>,

"priority":<Integer_value>,

"gotopriorityexpression":<String_value>,

"bindpoint":<String_value>,

"invoke":<Boolean_value>,

"labeltype":<String_value>,

"labelname":<String_value>
```

```
}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/crvserver_cmppolicy_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ crvserver_cmppolicy_binding/ name_value<String> ? **args=policyname: <String_value> ,bindpoint: <String_value> ,priority: <Integer_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/crvserver_cmppolicy_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ crvserver_cmppolicy_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of crvserver_cmppolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/crvserver_cmppolicy_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the crvserver_cmppolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "crvserver_cmppolicy_binding": [ {

"labelname":<String_value>,

"name":<String_value>,

"bindpoint":<String_value>,

"priority":<Integer_value>,

"labeltype":<String_value>,

"policyname":<String_value>,

"invoke":<Boolean_value>,

"gotopriorityexpression":<String_value>,

"targetvserver":<String_value>,

"inherited":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/crvserver_cmppolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ crvserver_cmppolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "crvserver_cmppolicy_binding": [ {

"labelname":<String_value>,

"name":<String_value>,

"bindpoint":<String_value>,

"priority":<Integer_value>,

"labeltype":<String_value>,

"policyname":<String_value>,

"invoke":<Boolean_value>,

"gotopriorityexpression":<String_value>,

"targetvserver":<String_value>,
```

```
"inherited":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/crvserver_cmppolicy_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"crvserver_cmppolicy_binding": [ { "__count": "#no"} ] }
```

crvserver_crpolicy_binding

Binding object showing the crpolicy that can be bound to crvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
priority	<Integer>	Read-write	The priority for the policy.
labeltype	<String>	Read-write	The invocation type.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = reqvserver, resvserver, policylabel
bindpoint	<String>	Read-write	The bindpoint to which the policy is bound. Possible values = REQUEST, RESPONSE, ICA_REQUEST
name	<String>	Read-write	Name of the cache redirection virtual server to which to bind the cache redirection policy. Minimum length = 1
labelname	<String>	Read-write	Name of the label invoked.
targetvserver	<String>	Read-write	Name of the virtual server to which content is forwarded. Applicable only if the policy is a map policy and the cache redirection virtual server is of type REVERSE. Minimum length = 1
policyname	<String>	Read-write	Policies bound to this vserver.
invoke	<Boolean>	Read-write	Invoke flag.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
gotopriorityexpression	<String>	Read-write	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
pipolicyhits	<Integer>	Read-only	Number of hits.
hits	<Integer>	Read-only	Number of hits.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/crvserver_crpolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"crvserver_crpolicy_binding":{

<b>"name":<String_value>,

</b>"policyname":<String_value>,

"targetvserver":<String_value>,

"priority":<Integer_value>,

"gotopriorityexpression":<String_value>,

"bindpoint":<String_value>,

"invoke":<Boolean_value>,

"labeltype":<String_value>,

"labelname":<String_value>
```

```
}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/crvserver_crpolicy_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ crvserver_crpolicy_binding/ name_value<String> ? **args=policyname: <String_value> ,bindpoint: <String_value> ,priority: <Integer_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/crvserver_crpolicy_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ crvserver_crpolicy_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of crvserver_crpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/crvserver_crpolicy_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the crvserver_crpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "crvserver_crpolicy_binding": [ {

"priority":<Integer_value>,

"labeltype":<String_value>,

"bindpoint":<String_value>,

"name":<String_value>,

"labelname":<String_value>,

"targetvserver":<String_value>,

"policyname":<String_value>,

"invoke":<Boolean_value>,

"gotopriorityexpression":<String_value>,

"pipolicyhits":<Integer_value>,

"hits":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/crvserver_crpolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/crvserver_crpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "crvserver_crpolicy_binding": [ {

"priority":<Integer_value>,

"labeltype":<String_value>,

"bindpoint":<String_value>,

"name":<String_value>,

"labelname":<String_value>,

"targetvserver":<String_value>,

"policyname":<String_value>,
```

```
"invoke":<Boolean_value>,

"gotopriorityexpression":<String_value>,

"pipolicyhits":<Integer_value>,

"hits":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/crvserver_crpolicy_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"crvserver_crpolicy_binding": [ { "__count": "#no"} ] }
```

crvserver_cspolicy_binding

Binding object showing the cspolicy that can be bound to crvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
invoke	<Boolean>	Read-write	Invoke flag.
gotopriorityexpression	<String>	Read-write	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
policyname	<String>	Read-write	Policies bound to this vserver.
targetvserver	<String>	Read-write	The CSW target server names.
labelname	<String>	Read-write	Name of the label invoked.
bindpoint	<String>	Read-write	The bindpoint to which the policy is bound. Possible values = REQUEST, RESPONSE, ICA_REQUEST
priority	<Integer>	Read-write	The priority for the policy.
labeltype	<String>	Read-write	The invocation type. Possible values = reqvserver, resvserver, policylabel
name	<String>	Read-write	Name of the cache redirection virtual server to which to

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			bind the cache redirection policy. Minimum length = 1
pipolicyhits	<Integer>	Read-only	Number of hits.
hits	<Integer>	Read-only	Number of hits.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/crvserver_cspolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"crvserver_cspolicy_binding":{

<b>"name":<String_value>,

</b>"policyname":<String_value>,

"targetvserver":<String_value>,

"priority":<Integer_value>,

"gotopriorityexpression":<String_value>,

"bindpoint":<String_value>,

"invoke":<Boolean_value>,

"labeltype":<String_value>,

"labelname":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/crvserver_cspolicy_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ crvserver_cspolicy_binding/ name_value<String> ? **args=policyname: <String_value> ,bindpoint: <String_value> ,priority: <Integer_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/crvserver_cspolicy_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ crvserver_cspolicy_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of crvserver_cspolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/crvserver_cspolicy_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the crvserver_cspolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "crvserver_cspolicy_binding": [ {

"invoke":<Boolean_value>,

"gotopriorityexpression":<String_value>,

"policyname":<String_value>,

"targetvserver":<String_value>,

"labelname":<String_value>,

"bindpoint":<String_value>,

"priority":<Integer_value>,

"labeltype":<String_value>,

"name":<String_value>,

"pipolicyhits":<Integer_value>,

"hits":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/crvserver_cspolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/crvserver_cspolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "crvserver_cspolicy_binding": [ {

"invoke":<Boolean_value>,

"gotopriorityexpression":<String_value>,

"policyname":<String_value>,

"targetvserver":<String_value>,

"labelname":<String_value>,

"bindpoint":<String_value>,

"priority":<Integer_value>,

"labeltype":<String_value>,

"name":<String_value>,

"pipolicyhits":<Integer_value>,
```

```
"hits":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/crvserver_cspolicy_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"crvserver_cspolicy_binding": [ { "__count": "#no"} ] }
```

crvserver_feopolicy_binding

Binding object showing the feopolicy that can be bound to crvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the cache redirection virtual server to which to

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			bind the cache redirection policy. Minimum length = 1
bindpoint	<String>	Read-write	The bindpoint to which the policy is bound. Possible values = REQUEST, RESPONSE, ICA_REQUEST
priority	<Integer>	Read-write	The priority for the policy.
labeltype	<String>	Read-write	Type of label to be invoked. Possible values = reqvserver, resvserver, policylabel
labelname	<String>	Read-write	Name of the label to be invoked.
targetvserver	<String>	Read-write	Name of the virtual server to which content is forwarded. Applicable only if the policy is a map policy and the cache redirection virtual server is of type REVERSE. Minimum length = 1
invoke	<Boolean>	Read-write	Invoke a policy label if this policy's rule evaluates to TRUE.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
gotopriorityexpression	<String>	Read-write	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
policyname	<String>	Read-write	Policies bound to this vserver.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/crvserver_feopolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"crvserver_feopolicy_binding":{

<b>"name":<String_value>,

</b>"policyname":<String_value>,

"targetvserver":<String_value>,

"priority":<Integer_value>,

"gotopriorityexpression":<String_value>,

"bindpoint":<String_value>,

"invoke":<Boolean_value>,

"labeltype":<String_value>,
```

```
"labelname":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/crvserver_feopolicy_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ crvserver_feopolicy_binding/ name_value<String> ? **args=policyname: <String_value> ,bindpoint: <String_value> ,priority: <Integer_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/crvserver_feopolicy_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ crvserver_feopolicy_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of crvserver_feopolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/crvserver_feopolicy_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the crvserver_feopolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "crvserver_feopolicy_binding": [ {

"name":<String_value>,

"bindpoint":<String_value>,

"priority":<Integer_value>,

"labeltype":<String_value>,

"labelname":<String_value>,

"targetvserver":<String_value>,

"invoke":<Boolean_value>,

"gotopriorityexpression":<String_value>,

"policyname":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/crvserver_feopolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ crvserver_feopolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "crvserver_feopolicy_binding": [ {

"name":<String_value>,

"bindpoint":<String_value>,

"priority":<Integer_value>,

"labeltype":<String_value>,

"labelname":<String_value>,

"targetvserver":<String_value>,

"invoke":<Boolean_value>,

"gotopriorityexpression":<String_value>,

"policyname":<String_value>
```

```
}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/crvserver_feopolicy_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"crvserver_feopolicy_binding": [ { "__count": "#no"} ] }
```

crvserver_icapolicy_binding

Binding object showing the icapolicy that can be bound to crvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
labelname	<String>	Read-write	Name of the label to be invoked.
name	<String>	Read-write	Name of the cache redirection virtual server to which to

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			bind the cache redirection policy. Minimum length = 1
labeltype	<String>	Read-write	Type of label to be invoked. Possible values = reqvserver, resvserver, policylabel
priority	<Integer>	Read-write	The priority for the policy.
bindpoint	<String>	Read-write	For a rewrite policy, the bind point to which to bind the policy. Note: This parameter applies only to rewrite policies, because content switching policies are evaluated only at request time. Possible values = REQUEST, RESPONSE, ICA_REQUEST
policyname	<String>	Read-write	Policies bound to this vserver.
gotopriorityexpression	<String>	Read-write	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
invoke	<Boolean>	Read-write	Invoke a policy label if this policy's rule evaluates to TRUE.
targetvserver	<String>	Read-write	Name of the virtual server to which content is forwarded. Applicable only if the policy is a map policy and the cache redirection virtual server is of type REVERSE. Minimum length = 1
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/crvserver_icapolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"crvserver_icapolicy_binding":{

<b>"name":<String_value>,

</b>"policyname":<String_value>,

"targetvserver":<String_value>,

"priority":<Integer_value>,

"gotopriorityexpression":<String_value>,

"bindpoint":<String_value>,
```

```
"invoke":<Boolean_value>,

"labeltype":<String_value>,

"labelname":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/crvserver_icapolicy_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ crvserver_icapolicy_binding/ name_value<String> ? **args=policyname: <String_value> ,bindpoint: <String_value> ,priority: <Integer_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/crvserver_icapolicy_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ crvserver_icapolicy_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of crvserver_icapolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/crvserver_icapolicy_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the crvserver_icapolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "crvserver_icapolicy_binding": [ {

"labelname":<String_value>,

"name":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"bindpoint":<String_value>,

"policyname":<String_value>,

"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>,

"targetvserver":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/crvserver_icapolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/crvserver_icapolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "crvserver_icapolicy_binding": [ {

"labelname":<String_value>,

"name":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"bindpoint":<String_value>,

"policyname":<String_value>,

"gotopriorityexpression":<String_value>,
```

```
"invoke":<Boolean_value>,

"targetvserver":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/crvserver_icapolicy_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"crvserver_icapolicy_binding": [ { "__count": "#no"} ] }
```

crvserver_lbvserver_binding

Binding object showing the lbvserver that can be bound to crvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
lbvserver	<String>	Read-write	The Default target server name.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum length = 1
name	<String>	Read-write	Name of the cache redirection virtual server to which to bind the cache redirection policy. Minimum length = 1
hits	<Integer>	Read-only	Number of hits.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.
- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/crvserver_lbvserver_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"crvserver_lbvserver_binding":{

<b>"name":<String_value>,

</b>"lbvserver":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/crvserver_lbvserver_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ crvserver_lbvserver_binding/ name_value<String> ? **args=lbvserver: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/crvserver_lbvserver_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ crvserver_lbvserver_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of crvserver_lbvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/crvserver_lbvserver_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the crvserver_lbvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "crvserver_lbvserver_binding": [ {

"lbvserver":<String_value>,

"name":<String_value>,

"hits":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/crvserver_lbvserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/crvserver_lbvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "crvserver_lbvserver_binding": [ {

"lbvserver":<String_value>,

"name":<String_value>,

"hits":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/crvserver_lbvserver_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"crvserver_lbvserver_binding": [ { "__count": "#no"} ] }
```

crvserver_policymap_binding

Binding object showing the policymap that can be bound to crvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
labelname	<String>	Read-write	Name of the label to be invoked.
priority	<Integer>	Read-write	An unsigned integer that determines the priority of the policy relative to other policies bound to this cache redirection virtual server. The lower the value, higher the priority. Note: This option is available only when binding content switching, filtering, and compression policies to a cache redirection virtual server.
labeltype	<String>	Read-write	Type of label to be invoked. Possible values = reqvserver, resvserver, policylabel
bindpoint	<String>	Read-write	For a rewrite policy, the bind point to which to bind the policy. Note: This parameter applies only to rewrite policies, because content switching policies are evaluated only at request time.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = REQUEST, RESPONSE, ICA_REQUEST
name	<String>	Read-write	Name of the cache redirection virtual server to which to bind the cache redirection policy. Minimum length = 1
policyname	<String>	Read-write	Policies bound to this vserver.
invoke	<Boolean>	Read-write	Invoke a policy label if this policy's rule evaluates to TRUE.
gotopriorityexpression	<String>	Read-write	Expression or other value specifying the next policy to be evaluated if the current policy evaluates to TRUE. Specify one of the following values: * NEXT - Evaluate the policy with the next higher priority number. * END - End policy evaluation. * USE_INVOCATION_RESULT - Applicable if this policy invokes another policy label. If the final goto in the invoked policy label has a value of END, the evaluation stops. If the final goto is

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			anything other than END, the current policy label performs a NEXT. * An expression that evaluates to a number. If you specify an expression, the number to which it evaluates determines the next policy to evaluate, as follows: * If the expression evaluates to a higher numbered priority, the policy with that priority is evaluated next. * If the expression evaluates to the priority of the current policy, the policy with the next higher numbered priority is evaluated next. * If the expression evaluates to a priority number that is numerically higher than the highest numbered priority, policy evaluation ends. An UNDEF event is triggered if: * The expression is invalid. * The expression evaluates to a priority number that is numerically lower

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			than the current policy's priority. * The expression evaluates to a priority number that is between the current policy's priority number (say, 30) and the highest priority number (say, 100), b ut does not match any configured priority number (for example, the expression evaluates to the number 85). This example assumes that the priority number incr ements by 10 for every successive policy, and therefore a priority number of 85 does not exist in the policy label.
targetvserver	<String>	Read-write	The CSW target server names.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/crvserver_policymap_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"crvserver_policymap_binding":{
```

```
<b>"name":<String_value>,

</b>"policyname":<String_value>,

"targetvserver":<String_value>,

"priority":<Integer_value>,

"gotopriorityexpression":<String_value>,

"bindpoint":<String_value>,

"invoke":<Boolean_value>,

"labeltype":<String_value>,

"labelname":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/crvserver_policymap_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ crvserver_policymap_binding/ name_value<String> ? **args=policyname: <String_value> ,bindpoint: <String_value> ,priority: <Integer_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/crvserver_policymap_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ crvserver_policymap_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of crvserver_policymap_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/crvserver_policymap_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the crvserver_policymap_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "crvserver_policymap_binding": [ {

"labelname":<String_value>,

"priority":<Integer_value>,

"labeltype":<String_value>,

"bindpoint":<String_value>,

"name":<String_value>,
```

```
"policyname":<String_value>,

"invoke":<Boolean_value>,

"gotopriorityexpression":<String_value>,

"targetvserver":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/crvserver_policymap_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/crvserver_policymap_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "crvserver_policymap_binding": [ {

"labelname":<String_value>,
```

```
"priority":<Integer_value>,

"labeltype":<String_value>,

"bindpoint":<String_value>,

"name":<String_value>,

"policyname":<String_value>,

"invoke":<Boolean_value>,

"gotopriorityexpression":<String_value>,

"targetvserver":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/crvserver_policymap_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"crvserver_policymap_binding": [ { "__count": "#no"} ] }
```

crvserver_responderpolicy_binding

Binding object showing the responderpolicy that can be bound to crvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
targetvserver	<String>	Read-write	Name of the virtual server to which content is forwarded. Applicable only if the policy is a map policy and the cache redirection virtual server is of type REVERSE. Minimum length = 1
policyname	<String>	Read-write	Policies bound to this vserver.
invoke	<Boolean>	Read-write	Invoke flag.
gotopriorityexpression	<String>	Read-write	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
name	<String>	Read-write	Name of the cache redirection virtual server to which to bind the cache redirection policy. Minimum length = 1
bindpoint	<String>	Read-write	For a rewrite policy, the bind point to which to bind the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			policy. Note: This parameter applies only to rewrite policies, because content switching policies are evaluated only at request time. Possible values = REQUEST, RESPONSE, ICA_REQUEST
priority	<Integer>	Read-write	The priority for the policy.
labeltype	<String>	Read-write	The invocation type. Possible values = reqvserver, resvserver, policylabel
labelname	<String>	Read-write	Name of the label invoked.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/crvserver_responderpolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"crvserver_responderpolicy_binding":{

<b>"name":<String_value>,
```

```
</b>"policyname":<String_value>,

"targetvserver":<String_value>,

"priority":<Integer_value>,

"gotopriorityexpression":<String_value>,

"bindpoint":<String_value>,

"invoke":<Boolean_value>,

"labeltype":<String_value>,

"labelname":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/crvserver_responderpolicy_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ crvserver_responderpolicy_binding/ name_value<String> ? **args=policyname: <String_value> ,bindpoint: <String_value> ,priority: <Integer_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/crvserver_responderpolicy_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ crvserver_responderpolicy_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of crvserver_responderpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/crvserver_responderpolicy_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the crvserver_responderpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "crvserver_responderpolicy_binding": [ {

"targetvserver":<String_value>,

"policyname":<String_value>,

"invoke":<Boolean_value>,

"gotopriorityexpression":<String_value>,

"name":<String_value>,
```

```
"bindpoint":<String_value>,

"priority":<Integer_value>,

"labeltype":<String_value>,

"labelname":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/crvserver_responderpolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/crvserver_responderpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "crvserver_responderpolicy_binding": [ {

"targetvserver":<String_value>,
```

```
"policyname":<String_value>,

"invoke":<Boolean_value>,

"gotopriorityexpression":<String_value>,

"name":<String_value>,

"bindpoint":<String_value>,

"priority":<Integer_value>,

"labeltype":<String_value>,

"labelname":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/crvserver_responderpolicy_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"crvserver_responderpolicy_binding": [ { "__count": "#no"} ] }
```

crvserver_rewritepolicy_binding

Binding object showing the rewritepolicy that can be bound to crvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
targetvserver	<String>	Read-write	Name of the virtual server to which content is forwarded. Applicable only if the policy is a map policy and the cache redirection virtual server is of type REVERSE. Minimum length = 1
gotopriorityexpression	<String>	Read-write	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
invoke	<Boolean>	Read-write	Invoke flag.
policyname	<String>	Read-write	Policies bound to this vserver.
labeltype	<String>	Read-write	The invocation type. Possible values = reqvserver, resvserver, policylabel
priority	<Integer>	Read-write	The priority for the policy.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
bindpoint	<String>	Read-write	The bindpoint to which the policy is bound. Possible values = REQUEST, RESPONSE, ICA_REQUEST
name	<String>	Read-write	Name of the cache redirection virtual server to which to bind the cache redirection policy. Minimum length = 1
labelname	<String>	Read-write	Name of the label invoked.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/crvserver_rewritepolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"crvserver_rewritepolicy_binding":{

<b>"name":<String_value>,

</b>"policyname":<String_value>,

"targetvserver":<String_value>,

"priority":<Integer_value>,
```

```
"gotopriorityexpression":<String_value>,

"bindpoint":<String_value>,

"invoke":<Boolean_value>,

"labeltype":<String_value>,

"labelname":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/crvserver_rewritepolicy_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ crvserver_rewritepolicy_binding/ name_value<String> ? **args=policyname: <String_value> ,bindpoint: <String_value> ,priority: <Integer_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/crvserver_rewritepolicy_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ crvserver_rewritepolicy_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of crvserver_rewritepolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/crvserver_rewritepolicy_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the crvserver_rewritepolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "crvserver_rewritepolicy_binding": [ {

"targetvserver":<String_value>,

"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>,

"policyname":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"bindpoint":<String_value>,

"name":<String_value>,
```

```
"labelname":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/crvserver_rewritepolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/crvserver_rewritepolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "crvserver_rewritepolicy_binding": [ {

"targetvserver":<String_value>,

"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>,

"policyname":<String_value>,
```

```
"labeltype":<String_value>,

"priority":<Integer_value>,

"bindpoint":<String_value>,

"name":<String_value>,

"labelname":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/crvserver_rewritepolicy_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"crvserver_rewritepolicy_binding": [ { "__count": "#no"} ] }
```

crvserver_spilloverpolicy_binding

Binding object showing the spilloverpolicy that can be bound to crvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
targetvserver	<String>	Read-write	Name of the virtual server to which content is forwarded. Applicable only if the policy is a map policy and the cache redirection virtual server is of type REVERSE. Minimum length = 1
gotopriorityexpression	<String>	Read-write	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
invoke	<Boolean>	Read-write	Invoke a policy label if this policy's rule evaluates to TRUE.
policyname	<String>	Read-write	Policies bound to this vserver.
name	<String>	Read-write	Name of the cache redirection virtual server to which to bind the cache redirection policy. Minimum length = 1
bindpoint	<String>	Read-write	The bindpoint to which the policy is bound.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = REQUEST, RESPONSE, ICA_REQUEST
labeltype	<String>	Read-write	Type of label to be invoked. Possible values = reqvserver, resvserver, policylabel
priority	<Integer>	Read-write	The priority for the policy.
labelname	<String>	Read-write	Name of the label to be invoked.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/crvserver_spilloverpolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"crvserver_spilloverpolicy_binding":{

<b>"name":<String_value>,

</b>"policyname":<String_value>,

"targetvserver":<String_value>,

"priority":<Integer_value>,
```

```
"gotopriorityexpression":<String_value>,

"bindpoint":<String_value>,

"invoke":<Boolean_value>,

"labeltype":<String_value>,

"labelname":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/crvserver_spilloverpolicy_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ crvserver_spilloverpolicy_binding/ name_value<String> ? **args=policyname: <String_value> ,bindpoint: <String_value> ,priority: <Integer_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/crvserver_spilloverpolicy_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ crvserver_spilloverpolicy_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of crvserver_spilloverpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/crvserver_spilloverpolicy_binding/name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the crvserver_spilloverpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "crvserver_spilloverpolicy_binding": [ {

"targetvserver":<String_value>,

"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>,

"policyname":<String_value>,

"name":<String_value>,

"bindpoint":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,
```

```
"labelname":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/crvserver_spilloverpolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/crvserver_spilloverpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "crvserver_spilloverpolicy_binding": [ {

"targetvserver":<String_value>,

"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>,

"policyname":<String_value>,
```

```
"name":<String_value>,

"bindpoint":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"labelname":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/crvserver_spilloverpolicy_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"crvserver_spilloverpolicy_binding": [ { "__count": "#no"} ] }
```

cs

Content Switching

Content Switching configuration. Content Switching feature that enables you to direct traffic to servers on the basis of content.

NAME	DESCRIPTION
csaction	Configuration for Content Switching action
csparameter	Configuration for CS parameter
cspolicy	Configuration for content-switching policy
cspolicy_binding	Binding object showing the resources that can be bound to cspolicy
cspolicy_crvserver_binding	Binding object showing the crvserver that can be bound to cspolicy
cspolicy_cspolicylabel_binding	Binding object showing the cspolicylabel that can be bound to cspolicy
cspolicy_csvserver_binding	Binding object showing the csvserver that can be bound to cspolicy
cspolicylabel	Configuration for CS policy label
cspolicylabel_binding	Binding object showing the resources that can be bound to cspolicylabel
cspolicylabel_cspolicy_binding	Binding object showing the cspolicy that can be bound to cspolicylabel

NAME	DESCRIPTION
csvserver	Configuration for CS virtual server
csvserver_analyticsprofile_binding	Binding object showing the analyticsprofile that can be bound to csvserver
csvserver_appflowpolicy_binding	Binding object showing the appflowpolicy that can be bound to csvserver
csvserver_appfwpolicy_binding	Binding object showing the appfwpolicy that can be bound to csvserver
csvserver_appqoepolicy_binding	Binding object showing the appqoepolicy that can be bound to csvserver
csvserver_auditnslogpolicy_binding	Binding object showing the auditnslogpolicy that can be bound to csvserver
csvserver_auditsyslogpolicy_binding	Binding object showing the auditsyslogpolicy that can be bound to csvserver
csvserver_authorizationpolicy_binding	Binding object showing the authorizationpolicy that can be bound to csvserver
csvserver_binding	Binding object showing the resources that can be bound to csvserver
csvserver_botpolicy_binding	Binding object showing the botpolicy that can be bound to csvserver

NAME	DESCRIPTION
csvserver_cachepolicy_binding	Binding object showing the cachepolicy that can be bound to csvserver
csvserver_cmppolicy_binding	Binding object showing the cmppolicy that can be bound to csvserver
csvserver_contentinspectionpolicy_binding	Binding object showing the contentinspectionpolicy that can be bound to csvserver
csvserver_cspolicy_binding	Binding object showing the cspolicy that can be bound to csvserver
csvserver_domain_binding	Binding object showing the domain that can be bound to csvserver
csvserver_feopolicy_binding	Binding object showing the feopolicy that can be bound to csvserver
csvserver_gslbvserver_binding	Binding object showing the gslbvserver that can be bound to csvserver
csvserver_lbvserver_binding	Binding object showing the lbvserver that can be bound to csvserver
csvserver_responderpolicy_binding	Binding object showing the responderpolicy that can be bound to csvserver
csvserver_rewritepolicy_binding	Binding object showing the rewritepolicy that can be bound to csvserver

NAME	DESCRIPTION
csvserver_spilloverpolicy_binding	Binding object showing the spilloverpolicy that can be bound to csvserver
csvserver_tmtrafficpolicy_binding	Binding object showing the tmtrafficpolicy that can be bound to csvserver
csvserver_transformpolicy_binding	Binding object showing the transformpolicy that can be bound to csvserver
csvserver_vpnvserver_binding	Binding object showing the vpnvserver that can be bound to csvserver

csaction

Configuration for Content Switching action resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the content switching action. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at sign (@), equal sign (=), and hyphen (-) characters. Can be changed after the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			content switching action is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my action" or 'my action').
targetlbvserver	<String>	Read-write	Name of the load balancing virtual server to which the content is switched.
targetvserver	<String>	Read-write	Name of the VPN, GSLB or Authentication virtual server to which the content is switched.
targetvserverexpr	<String>	Read-write	Information about this content switching action. Maximum length = 1499
comment	<String>	Read-write	Comments associated with this cs action.
newname	<String>	Read-write	New name for the content switching action. Must begin

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at sign (@), equal sign (=), and hyphen (-) characters. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my name" or 'my name'). Minimum length = 1
hits	<Integer>	Read-only	The number of times the action has been taken.
referencecount	<Integer>	Read-only	The number of references to the action.
undefhits	<Integer>	Read-only	The number of times the action resulted in UNDEF.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
builtin	<String[]>	Read-only	. Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL
feature	<String>	Read-only	The feature to be checked while applying this config.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT
- RENAME

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/csaction **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"csaction":{

<b>"name":<String_value>,

</b>"targetlbvserver":<String_value>,

"targetvserver":<String_value>,

"targetvserverexpr":<String_value>,

"comment":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/csaction/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/csaction **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"csaction":{

<b>"name":<String_value>,

</b>"targetlbvserver":<String_value>,

"targetvserver":<String_value>,

"targetvserverexpr":<String_value>,

"comment":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/csaction? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"csaction":{

<b>"name":<String_value>,

</b>"comment":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

RENAME

URL: http:// <netscaler-ip-address> /nitro/v1/config/csaction? **action=rename HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"csaction":{

<b>"name":<String_value>,

</b><b>"newname":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/csaction **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/csaction? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/csaction? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of csaction resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/csaction? **view=summary**

Use this query-parameter to get the summary output of csaction resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/csaction? **pagesize=#no;pageno=#no**

Use this query-parameter to get the csaction resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "csaction": [ {

"name":<String_value>,

"targetlbvserver":<String_value>,

"targetvserver":<String_value>,

"targetvserverexpr":<String_value>,

"hits":<Integer_value>,

"referencecount":<Integer_value>,

"undefhits":<Integer_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"comment":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/csaction/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/csaction/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/csaction/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of csaction resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "csaction": [ {

"name":<String_value>,

"targetlbvserver":<String_value>,

"targetvserver":<String_value>,

"targetvserverexpr":<String_value>,

"hits":<Integer_value>,

"referencecount":<Integer_value>,

"undefhits":<Integer_value>,
```

```
"builtin":<String[]_value>,

"feature":<String_value>,

"comment":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/csaction? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "csaction": [ { "__count": "#no"} ] }
```

csparameter

Configuration for CS parameter resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
stateupdate	<String>	Read-write	Specifies whether the virtual server checks the attached load balancing server for state information. Default value: DISABLED Possible values = ENABLED, DISABLED
builtin	<String[]>	Read-only	Flag to determine if CS param is built-in or not. Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL
feature	<String>	Read-only	The feature to be checked while applying this config.
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- UPDATE
- UNSET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/csparameter **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"csparameter":{

"stateupdate":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/csparameter? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"csparameter":{

"stateupdate":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/csparameter **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "csparameter": [ {

"stateupdate":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

cspolicy

Configuration for content-switching policy resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
policyname	<String>	Read-write	Name for the content switching policy. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at sign (@), equal sign (=), and hyphen (-) characters. Cannot

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			be changed after a policy is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my policy" or 'my policy'). Minimum length = 1
rule	<String>	Read-write	Expression, or name of a named expression, against which traffic is evaluated. The following requirements apply only to the Citrix ADC CLI: * If the expression includes one or more spaces, enclose the entire expression in double quotation marks. * If the expression itself includes double quotation

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			marks, escape the quotations by using the character. * Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks.
action	<String>	Read-write	Content switching action that names the target load balancing virtual server to which the traffic is switched.
logaction	<String>	Read-write	The log action associated with the content switching policy.
newname	<String>	Read-write	The new name of the content switching policy. Minimum length = 1
vstype	<Integer>	Read-only	Virtual server type.
hits	<Integer>	Read-only	Total number of hits.
labelname	<String>	Read-only	Name of the label invoked.
labeltype	<String>	Read-only	The invocation type. Possible values = reqvserver,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			resvserver, policylabel
priority	<Integer>	Read-only	priority of bound policy.
activepolicy	<Boolean>	Read-only	Indicates whether policy is bound or not.
boundto	<String>	Read-only	Location where policy is bound. Minimum length = 1
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT
- RENAME

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/cspolicy **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"cspolicy":{

<b>"policyname":<String_value>,

</b><b>"rule":<String_value>,

</b>"action":<String_value>,

"logaction":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/cspolicy/ policyname_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/cspolicy **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"cspolicy":{

<b>"policyname":<String_value>,

</b>"rule":<String_value>,

"action":<String_value>,

"logaction":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/cspolicy? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"cspolicy":{

<b>"policyname":<String_value>,

</b>"logaction":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

RENAME

URL: http:// <netscaler-ip-address> /nitro/v1/config/cspolicy? **action=rename HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"cspolicy":{

<b>"policyname":<String_value>,

</b><b>"newname":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/cspolicy **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/cspolicy? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/cspolicy? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of cspolicy resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/cspolicy? **view=summary**

Use this query-parameter to get the summary output of cspolicy resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/cspolicy? **pagesize=#no;pageno=#no**

Use this query-parameter to get the cspolicy resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "cspolicy": [ {

"policyname":<String_value>,

"rule":<String_value>,

"action":<String_value>,

"vstype":<Integer_value>,

"hits":<Integer_value>,

"labelname":<String_value>,

"labeltype":<String_value>,

"target":<String_value>,

"priority":<Integer_value>,

"activepolicy":<Boolean_value>,

"logaction":<String_value>,

"boundto":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/cspolicy/ policyname_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/cspolicy/ policyname_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/cspolicy/ policyname_value<String> ? **view=summary**

Use this query-parameter to get the summary output of cspolicy resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "cspolicy": [ {

"policyname":<String_value>,

"rule":<String_value>,

"action":<String_value>,

"vstype":<Integer_value>,
```

```
"hits":<Integer_value>,

"labelname":<String_value>,

"labeltype":<String_value>,

"target":<String_value>,

"priority":<Integer_value>,

"activepolicy":<Boolean_value>,

"logaction":<String_value>,

"boundto":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/cspolicy? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "cspolicy": [ { "__count": "#no"} ] }
```

cspolicy_binding

Binding object which returns the resources bound to cspolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
policyname	<String>	Read-write	Name of the content switching policy to display. If this parameter is omitted, details of all the policies are displayed. Minimum length = 1
cspolicy_csvserver_binding	<cspolicy_csvserver_binding[]>	Read-only	csvserver that can be bound to cspolicy.
cspolicy_cspolicylabel_binding	<cspolicy_cspolicylabel_binding[]>	Read-only	cspolicylabel that can be bound to cspolicy.
cspolicy_crvserver_binding	<cspolicy_crvserver_binding[]>	Read-only	crvserver that can be bound to cspolicy.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/cspolicy_binding/ policyname_value<String>
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "cspolicy_binding": [ {

"policyname":<String_value>,

"cspolicy_csvserver_binding":<cspolicy_csvserver_binding[]_value>,

"cspolicy_crvserver_binding":<cspolicy_crvserver_binding[]_value>,

"cspolicy_cspolicylabel_binding":<cspolicy_cspolicylabel_binding[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/cspolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/cspolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "cspolicy_binding": [ {

"policyname":<String_value>,

"cspolicy_csvserver_binding":<cspolicy_csvserver_binding[]_value>,

"cspolicy_crvserver_binding":<cspolicy_crvserver_binding[]_value>,

"cspolicy_cspolicylabel_binding":<cspolicy_cspolicylabel_binding[]_value>

}]}
```

cspolicy_crvserver_binding

Binding object showing the crvserver that can be bound to cspolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
boundto	<String>	Read-write	Location where policy is bound. Minimum length = 1
policyname	<String>	Read-write	Name of the content switching policy to display. If this parameter is omitted, details of all the policies are displayed. Minimum length = 1
labelname	<String>	Read-only	Name of the label invoked.
gotopriorityexpression	<String>	Read-only	Expression specifying the priority of the next policy which will get

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			evaluated if the current policy rule evaluates to TRUE. Minimum length = 1 Maximum length = 208
labeltype	<String>	Read-only	The invocation type. Possible values = reqvserver, resvserver, policylabel
priority	<Integer>	Read-only	priority of bound policy.
hits	<Integer>	Read-only	Total number of hits.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/cspolicy_crvserver_binding/ policyname_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ cspolicy_crvserver_binding/ policyname_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of cspolicy_crvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/cspolicy_crvserver_binding/ policyname_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the cspolicy_crvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "cspolicy_crvserver_binding": [ {

"boundto":<String_value>,

"policyname":<String_value>,

"labelname":<String_value>,

"gotopriorityexpression":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"hits":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/cspolicy_crvserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/cspolicy_crvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "cspolicy_crvserver_binding": [ {

"boundto":<String_value>,

"policyname":<String_value>,

"labelname":<String_value>,

"gotopriorityexpression":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"hits":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/cspolicy_crvserver_binding/ policyname_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"cspolicy_crvserver_binding": [ { "__count": "#no"} ] }
```

cspolicy_cspolicylabel_binding

Binding object showing the cspolicylabel that can be bound to cspolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
boundto	<String>	Read-write	Location where policy is bound. Minimum length = 1
policyname	<String>	Read-write	Name of the content switching policy to display. If this parameter is omitted, details of all the policies are displayed. Minimum length = 1
hits	<Integer>	Read-only	Total number of hits.
labeltype	<String>	Read-only	The invocation type. Possible values = reqvserver, resvserver, policylabel
priority	<Integer>	Read-only	priority of bound policy.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
labelname	<String>	Read-only	Name of the label invoked.
gotopriorityexpression	<String>	Read-only	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE. Minimum length = 1 Maximum length = 208
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/cspolicy_cspolicylabel_binding/ policyname_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ cspolicy_cspolicylabel_binding/ policyname_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of cspolicy_cspolicylabel_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/cspolicy_cspolicylabel_binding/ policyname_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the cspolicy_cspolicylabel_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "cspolicy_cspolicylabel_binding": [ {

"boundto":<String_value>,

"policyname":<String_value>,

"hits":<Integer_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"labelname":<String_value>,

"gotopriorityexpression":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/cspolicy_cspolicylabel_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/cspolicy_cspolicylabel_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "cspolicy_cspolicylabel_binding": [ {

"boundto":<String_value>,

"policyname":<String_value>,

"hits":<Integer_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"labelname":<String_value>,

"gotopriorityexpression":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/cspolicy_cspolicylabel_binding/ policyname_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"cspolicy_cspolicylabel_binding": [ { "__count": "#no"} ] }
```

cspolicy_csvserver_binding

Binding object showing the csvserver that can be bound to cspolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
policyname	<String>	Read-write	Name of the content switching policy to display. If this parameter is omitted, details of all the policies are displayed. Minimum length = 1
boundto	<String>	Read-write	Location where policy is bound. Minimum length = 1
labelname	<String>	Read-only	Name of the label invoked.
gotopriorityexpression	<String>	Read-only	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE. Minimum length = 1 Maximum length = 208
bindhits	<Integer>	Read-only	Total number of bind hits.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
hits	<Integer>	Read-only	Total number of hits.
action	<String>	Read-only	Content switching action that names the target load balancing virtual server to which the traffic is switched.
labeltype	<String>	Read-only	The invocation type. Possible values = reqvserver, resvserver, policylabel
priority	<Integer>	Read-only	priority of bound policy.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/cspolicy_csvserver_binding/ policyname_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/cspolicy_csvserver_binding/ policyname_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of cspolicy_csvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/cspolicy_csvserver_binding/ policyname_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the cspolicy_csvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "cspolicy_csvserver_binding": [ {

"policyname":<String_value>,

"boundto":<String_value>,

"labelname":<String_value>,

"gotopriorityexpression":<String_value>,

"bindhits":<Integer_value>,

"hits":<Integer_value>,

"action":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/cspolicy_csvserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/cspolicy_csvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "cspolicy_csvserver_binding": [ {

"policyname":<String_value>,

"boundto":<String_value>,

"labelname":<String_value>,

"gotopriorityexpression":<String_value>,

"bindhits":<Integer_value>,

"hits":<Integer_value>,

"action":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/cspolicy_csvserver_binding/ policyname_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"cspolicy_csvserver_binding": [ { "__count": "#no"} ] }
```

cspolicylabel

Configuration for CS policy label resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
labelname	<String>	Read-write	Name for the policy label. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at sign (@), equal sign (=), and hyphen (-) characters. The label name must be unique within the list of

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			policy labels for content switching. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my policylabel" or 'my policylabel').
cspolicylabeltype	<String>	Read-write	Protocol supported by the policy label. All policies bound to the policy label must either match the specified protocol or be a subtype of that protocol. Available settings function as follows: * HTTP - Supports policies that process HTTP traffic. Used to access unencrypted Web sites. (The default.) * SSL - Supports policies that process HTTPS/ SSL encrypted

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			traffic. Used to access encrypted Web sites. * TCP - Supports policies that process any type of TCP traffic, including HTTP. * SSL_TCP - Supports policies that process SSL-encrypted TCP traffic, including SSL. * UDP - Supports policies that process any type of UDP-based traffic, including DNS. * DNS - Supports policies that process DNS traffic. * ANY - Supports all types of policies except HTTP, SSL, and TCP. * SIP_UDP - Supports policies that process UDP based Session Initiation Protocol (SIP) traffic. SIP

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			initiates, manages, and terminates multimedia communications sessions, and has emerged as the standard for Internet telephony (VoIP). * RTSP - Supports policies that process Real Time Streaming Protocol (RTSP) traffic. RTSP provides delivery of multimedia and other streaming data, such as audio, video, and other types of streamed media. * RADIUS - Supports policies that process Remote Authentication Dial In User Service (RADIUS) traffic. RADIUS supports combined authentication, authorization, and auditing services for

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			network management. * MYSQL - Supports policies that process MYSQL traffic. * MSSQL - Supports policies that process Microsoft SQL traffic. Possible values = HTTP, TCP, RTSP, SSL, SSL_TCP, UDP, DNS, SIP_UDP, SIP_TCP, ANY, RADIUS, RDP, MYSQL, MSSQL, ORACLE, DIAMETER, SSL_DIAMETER, FTP, DNS_TCP, SMPP, MQTT, MQTT_TLS, HTTP_QUIC
newname	<String>	Read-write	The new name of the content switching policylabel. Minimum length = 1
numpol	<Integer>	Read-only	number of polices bound to label.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
hits	<Integer>	Read-only	Number of times policy label was invoked.
policyname	<String>	Read-only	Name of the content switching policy.
priority	<Integer>	Read-only	Specifies the priority of the policy.
targetvserver	<String>	Read-only	Name of the virtual server to which to forward requests that match the policy.
gotopriorityexpression	<String>	Read-only	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
labeltype	<String>	Read-only	Type of policy label invocation. Possible values = policylabel
invoke_labelname	<String>	Read-only	Name of the label to invoke if the current policy rule evaluates to TRUE.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD

- DELETE
- GET (ALL)
- GET
- COUNT
- RENAME

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/cspolicylabel **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"cspolicylabel":{

<b>"labelname":<String_value>,

</b><b>"cspolicylabeltype":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/cspolicylabel/ labelname_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

RENAME

URL: http:// <netscaler-ip-address> /nitro/v1/config/cspolicylabel? **action=rename HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"cspolicylabel":{

<b>"labelname":<String_value>,

</b><b>"newname":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/cspolicylabel **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/cspolicylabel? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/cspolicylabel? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of cspolicylabel resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/cspolicylabel? **view=summary**

Use this query-parameter to get the summary output of cspolicylabel resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/cspolicylabel? **pagesize=#no;pageno=#no**

Use this query-parameter to get the cspolicylabel resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "cspolicylabel": [ {

"labelname":<String_value>,

"cspolicylabeltype":<String_value>,

"numpol":<Integer_value>,

"hits":<Integer_value>,

"policyname":<String_value>,

"priority":<Integer_value>,

"targetvserver":<String_value>,

"gotopriorityexpression":<String_value>,

"labeltype":<String_value>,

"invoke_labelname":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/cspolicylabel/ labelname_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/cspolicylabel/ labelname_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/cspolicylabel/ labelname_value<String> ? **view=summary**

Use this query-parameter to get the summary output of cspolicylabel resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "cspolicylabel": [ {

"labelname":<String_value>,

"cspolicylabeltype":<String_value>,

"numpol":<Integer_value>,

"hits":<Integer_value>,
```

```
"policyname":<String_value>,

"priority":<Integer_value>,

"targetvserver":<String_value>,

"gotopriorityexpression":<String_value>,

"labeltype":<String_value>,

"invoke_labelname":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/cspolicylabel? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "cspolicylabel": [ { "__count": "#no"} ] }
```

cspolicylabel_binding

Binding object which returns the resources bound to cspolicylabel.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
labelname	<String>	Read-write	Name of the content switching policy label to display.
cspolicylabel_cspolicy_binding	<cspolicylabel_cspolicy_binding[]>	Read-only	cspolicy that can be bound to cspolicylabel.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/cspolicylabel_binding/ labelname_value<String>

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "cspolicylabel_binding": [ {

"labelname":<String_value>,

"cspolicylabel_cspolicy_binding":<cspolicylabel_cspolicy_binding[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/cspolicylabel_binding

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters:

bulkbindings

http:// <netscaler-ip-address> /nitro/v1/config/cspolicylabel_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "cspolicylabel_binding": [ {

"labelname":<String_value>,

"cspolicylabel_cspolicy_binding":<cspolicylabel_cspolicy_binding[]_value>

}]}
```

cspolicylabel_cspolicy_binding

Binding object showing the cspolicy that can be bound to cspolicylabel.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
targetvserver	<String>	Read-write	Name of the virtual server to which to forward requests that match the policy.
policyname	<String>	Read-write	Name of the content switching policy.
gotopriorityexpression	<String>	Read-write	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
invoke	<Boolean>	Read-write	.
invoke_labelname	<String>	Read-write	Name of the label to invoke if the current policy rule evaluates to TRUE.
labeltype	<String>	Read-write	Type of policy label invocation. Possible values = policylabel
priority	<Integer>	Read-write	Specifies the priority of the policy.
labelname	<String>	Read-write	Name of the policy label to which to bind a content switching policy.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/cspolicylabel_cspolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"cspolicylabel_cspolicy_binding":{

<b>"labelname":<String_value>,

</b><b>"policyname":<String_value>,

</b><b>"priority":<Integer_value>,

</b>"targetvserver":<String_value>,

"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>,

"labeltype":<String_value>,

"invoke_labelname":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/cspolicylabel_cspolicy_binding/ labelname_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ cspolicylabel_cspolicy_binding/ labelname_value<String> ? **args= policyname:<String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/cspolicylabel_cspolicy_binding/ labelname_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ cspolicylabel_cspolicy_binding/ labelname_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of cspolicylabel_cspolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/cspolicylabel_cspolicy_binding/ labelname_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the cspolicylabel_cspolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "cspolicylabel_cspolicy_binding": [ {

"targetvserver":<String_value>,
```

```
"policyname":<String_value>,

"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>,

"invoke_labelname":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"labelname":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/cspolicylabel_cspolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/cspolicylabel_cspolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "cspolicylabel_cspolicy_binding": [ {

"targetvserver":<String_value>,

"policyname":<String_value>,

"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>,

"invoke_labelname":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"labelname":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/cspolicylabel_cspolicy_binding/ labelname_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"cspolicylabel_cspolicy_binding": [ { "__count": "#no"} ] }
```

csvserver

Configuration for CS virtual server resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the content switching virtual server. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at sign (@), equal sign (=), and hyphen (-) characters. Cannot be changed after the CS virtual server is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			marks (for example, my server or my server). Minimum length = 1
td	<Integer>	Read-write	Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0. Minimum value = 0 Maximum value = 4094
servicetype	<String>	Read-write	Protocol used by the virtual server. Possible values = HTTP, SSL, TCP, FTP, RTSP, SSL_TCP, UDP, DNS, SIP_UDP, SIP_TCP, SIP_SSL, ANY, RADIUS, RDP, MYSQL, MSSQL, DIAMETER, SSL_DIAMETER, DNS_TCP, ORACLE, SMPP, PROXY, MONGO, MONGO_TLS,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			MQTT, MQTT_TLS, HTTP_QUIC, DOT, SSL_PROXY
ipv46	<String>	Read-write	IP address of the content switching virtual server. Minimum length = 1
targettype	<String>	Read-write	Virtual server target type. Possible values = GSLB
dnsrecordtype	<String>	Read-write	. Default value: NSGSLB_IPV4 Possible values = A, AAAA, CNAME, NAPTR
persistenceid	<Integer>	Read-write	. Minimum value = 0 Maximum value = 65535
ippattern	<String>	Read-write	IP address pattern, in dotted decimal notation, for identifying packets to be accepted by the virtual server. The IP Mask parameter specifies which part of the destination IP address is matched against the pattern. Mutually exclusive

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			with the IP Address parameter. For example, if the IP pattern assigned to the virtual server is 198.51.100.0 and the IP mask is 255.255.240.0 (a forward mask), the first 20 bits in the destination IP addresses are matched with the first 20 bits in the pattern. The virtual server accepts requests with IP addresses that range from 198.51.96.1 to 198.51.111.254. You can also use a pattern such as 0.0.2.2 and a mask such as 0.0.255.255 (a reverse mask). If a destination IP address matches more than one IP pattern, the pattern with the longest match is selected, and the associated virtual server processes the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			request. For example, if the virtual servers, vs1 and vs2, have the same IP pattern, 0.0.100.128, but different IP masks of 0.0.255.255 and 0.0.224.255, a destination IP address of 198.51.100.128 has the longest match with the IP pattern of vs1. If a destination IP address matches two or more virtual servers to the same extent, the request is processed by the virtual server whose port number matches the port number in the request.
ipmask	<String>	Read-write	IP mask, in dotted decimal notation, for the IP Pattern parameter. Can have leading or trailing non-zero octets (for example, 255.255.240.0 or 0.0.255.255). Accordingly, the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			mask specifies whether the first n bits or the last n bits of the destination IP address in a client request are to be matched with the corresponding bits in the IP pattern. The former is called a forward mask. The latter is called a reverse mask.
range	<Integer>	Read-write	Number of consecutive IP addresses, starting with the address specified by the IP Address parameter, to include in a range of addresses assigned to this virtual server. Default value: 1 Minimum value = 1 Maximum value = 254
port	<Integer>	Read-write	Port number for content switching virtual server. Minimum value = 1 Range 1 - 65535 * in CLI is represented as

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			65535 in NITRO API
ipset	<String>	Read-write	The list of IPv4/IPv6 addresses bound to ipset would form a part of listening service on the current cs vserver. Minimum length = 1
state	<String>	Read-write	Initial state of the load balancing virtual server. Default value: ENABLED Possible values = ENABLED, DISABLED
stateupdate	<String>	Read-write	Enable state updates for a specific content switching virtual server. By default, the Content Switching virtual server is always UP, regardless of the state of the Load Balancing virtual servers bound to it. This parameter interacts with the global setting as follows: Global Level | Vserver Level | Result

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			ENABLED ENABLED ENABLED ENABLED DISABLED ENABLED DISABLED ENABLED ENABLED DISABLED DISABLED DISABLED If you want to enable state updates for only some content switching virtual servers, be sure to disable the state update parameter. Default value: DISABLED Possible values = ENABLED, DISABLED, UPDATEONBACKENDUPDATE
cacheable	<String>	Read-write	Use this option to specify whether a virtual server, used for load balancing or content switching,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			routes requests to the cache redirection virtual server before sending it to the configured servers. Default value: NO Possible values = YES, NO
redirecturl	<String>	Read-write	URL to which traffic is redirected if the virtual server becomes unavailable. The service type of the virtual server should be either HTTP or SSL. Caution: Make sure that the domain in the URL does not match the domain specified for a content switching policy. If it does, requests are continuously redirected to the unavailable virtual server. Minimum length = 1
clttimeout	<Integer>	Read-write	Idle time, in seconds, after which the client connection is terminated. The default values are:

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			180 seconds for HTTP/SSL-based services. 9000 seconds for other TCP-based services. 120 seconds for DNS-based services. 120 seconds for other UDP-based services. Minimum value = 0 Maximum value = 31536000
precedence	<String>	Read-write	Type of precedence to use for both RULE-based and URL-based policies on the content switching virtual server. With the default (RULE) setting, incoming requests are evaluated against the rule-based content switching policies. If none of the rules match, the URL in the request is evaluated against the URL-based

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			content switching policies. Default value: RULE Possible values = RULE, URL
casesensitive	<String>	Read-write	Consider case in URLs (for policies that use URLs instead of RULES). For example, with the ON setting, the URLs /a/1.html and /A/1.HTML are treated differently and can have different targets (set by content switching policies). With the OFF setting, /a/1.html and /A/1.HTML are switched to the same target. Default value: ON Possible values = ON, OFF
somethod	<String>	Read-write	Type of spillover used to divert traffic to the backup virtual server when the primary virtual server reaches the spillover threshold. Connection spillover is based on the number of connections.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Bandwidth spillover is based on the total Kbps of incoming and outgoing traffic. Possible values = CONNECTION, DYNAMICCONNECTION, BANDWIDTH, HEALTH, LLMQUOTA, NONE
sopersistence	<String>	Read-write	Maintain source-IP based persistence on primary and backup virtual servers. Default value: DISABLED Possible values = ENABLED, DISABLED
sopersistencetimeout	<Integer>	Read-write	Time-out value, in minutes, for spillover persistence. Default value: 2 Minimum value = 2 Maximum value = 1440
sothreshold	<Integer>	Read-write	Depending on the spillover method, the maximum number of connections or the maximum total bandwidth (Kbps)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			that a virtual server can handle before spillover occurs. Minimum value = 1 Maximum value = 4294967287
sobackupaction	<String>	Read-write	Action to be performed if spillover is to take effect, but no backup chain to spillover is usable or exists. Possible values = DROP, ACCEPT, REDIRECT
redirectportrewrite	<String>	Read-write	State of port rewrite while performing HTTP redirect. Default value: DISABLED Possible values = ENABLED, DISABLED
downstateflush	<String>	Read-write	Flush all active transactions associated with a virtual server whose state transitions from UP to DOWN. Do not enable this option for applications that must complete their transactions.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: ENABLED Possible values = ENABLED, DISABLED
backupvserver	<String>	Read-write	Name of the backup virtual server that you are configuring. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at sign (@), equal sign (=), and hyphen (-) characters. Can be changed after the backup virtual server is created. You can assign a different backup virtual server or rename the existing virtual server. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			single quotation marks. Minimum length = 1
disableprimaryondown	<String>	Read-write	Continue forwarding the traffic to backup virtual server even after the primary server comes UP from the DOWN state. Default value: DISABLED Possible values = ENABLED, DISABLED
insertvserveripport	<String>	Read-write	Insert the virtual server's VIP address and port number in the request header. Available values function as follows: VIPADDR - Header contains the vserver's IP address and port number without any translation. OFF - The virtual IP and port header insertion option is disabled. V6TOV4MAPPING - Header contains the mapped IPv4

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			address corresponding to the IPv6 address of the vserver and the port number. An IPv6 address can be mapped to a user-specified IPv4 address using the set ns ip6 command. Possible values = OFF, VIPADDR, V6TOV4MAPPING
vipheader	<String>	Read-write	Name of virtual server IP and port header, for use with the VServer IP Port Insertion parameter. Minimum length = 1
rtspnat	<String>	Read-write	Enable network address translation (NAT) for real-time streaming protocol (RTSP) connections. Default value: OFF Possible values = ON, OFF
authenticationhost	<String>	Read-write	FQDN of the authentication virtual server. The service type of the virtual server should be either HTTP or SSL.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum length = 3 Maximum length = 252
authentication	<String>	Read-write	Authenticate users who request a connection to the content switching virtual server. Default value: OFF Possible values = ON, OFF
listenpolicy	<String>	Read-write	String specifying the listen policy for the content switching virtual server. Can be either the name of an existing expression or an in-line expression. Default value: "NONE"
listenpriority	<Integer>	Read-write	Integer specifying the priority of the listen policy. A higher number specifies a lower priority. If a request matches the listen policies of more than one virtual server the virtual server whose listen policy has the highest priority (the lowest priority

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			number) accepts the request. Default value: 101 Minimum value = 0 Maximum value = 100
authn401	<String>	Read-write	Enable HTTP 401-response based authentication. Default value: OFF Possible values = ON, OFF
authnvsname	<String>	Read-write	Name of authentication virtual server that authenticates the incoming user requests to this content switching virtual server. . Minimum length = 1 Maximum length = 252
push	<String>	Read-write	Process traffic with the push virtual server that is bound to this content switching virtual server (specified by the Push VServer parameter). The service type of the push virtual server

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			should be either HTTP or SSL. Default value: DISABLED Possible values = ENABLED, DISABLED
pushvserver	<String>	Read-write	Name of the load balancing virtual server, of type PUSH or SSL_PUSH, to which the server pushes updates received on the client-facing load balancing virtual server. Minimum length = 1
pushlabel	<String>	Read-write	Expression for extracting the label from the response received from server. This string can be either an existing rule name or an inline expression. The service type of the virtual server should be either HTTP or SSL. Default value: "none"
pushmulticlients	<String>	Read-write	Allow multiple Web 2.0 connections from the same client to connect to the virtual

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			server and expect updates. Default value: NO Possible values = YES, NO
tcpprofilename	<String>	Read-write	Name of the TCP profile containing TCP configuration settings for the virtual server. Minimum length = 1 Maximum length = 127
httpprofilename	<String>	Read-write	Name of the HTTP profile containing HTTP configuration settings for the virtual server. The service type of the virtual server should be either HTTP or SSL. Minimum length = 1 Maximum length = 127
dbprofilename	<String>	Read-write	Name of the DB profile. Minimum length = 1 Maximum length = 127
oracleserverversion	<String>	Read-write	Oracle server version.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: 10G Possible values = 10G, 11G
comment	<String>	Read-write	Information about this virtual server.
mssqlserverversion	<String>	Read-write	The version of the MSSQL server. Default value: 2008R2 Possible values = 70, 2000, 2000SP1, 2005, 2008, 2008R2, 2012, 2014
l2conn	<String>	Read-write	Use L2 Parameters to identify a connection. Possible values = ON, OFF
mysqlprotocolversion	<Integer>	Read-write	The protocol version returned by the mysql vserver. Default value: 10
mysqlserverversion	<String>	Read-write	The server version string returned by the mysql vserver. Minimum length = 1 Maximum length = 31

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
mysqlcharacterset	<Integer>	Read-write	The character set returned by the mysql vserver. Default value: 8
mysqlservercapabilities	<Integer>	Read-write	The server capabilities returned by the mysql vserver. Default value: 41613
appflowlog	<String>	Read-write	Enable logging appflow flow information. Default value: ENABLED Possible values = ENABLED, DISABLED
netprofile	<String>	Read-write	The name of the network profile. Minimum length = 1 Maximum length = 127
icmpvsrresponse	<String>	Read-write	Can be active or passive. Default value: PASSIVE Possible values = PASSIVE, ACTIVE
rhistate	<String>	Read-write	A host route is injected according to the setting on the virtual servers

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			* If set to PASSIVE on all the virtual servers that share the IP address, the appliance always injects the hostroute. * If set to ACTIVE on all the virtual servers that share the IP address, the appliance injects even if one virtual server is UP. * If set to ACTIVE on some virtual servers and PASSIVE on the others, the appliance, injects even if one virtual server set to ACTIVE is UP. Default value: PASSIVE Possible values = PASSIVE, ACTIVE
authnprofile	<String>	Read-write	Name of the authentication profile to be used when authentication is turned on.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
dnsprofilename	<String>	Read-write	Name of the DNS profile to be associated with the VServer. DNS profile properties will applied to the transactions processed by a VServer. This parameter is valid only for DNS and DNS-TCP VServers. Minimum length = 1 Maximum length = 127
dtls	<String>	Read-write	This option starts/stops the dtls service on the vserver. Default value: OFF Possible values = ON, OFF
persistencetype	<String>	Read-write	Type of persistence for the virtual server. Available settings function as follows: * SOURCEIP - Connections from the same client IP address belong to the same persistence session. * COOKIEINSERT - Connections that have the same

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			HTTP Cookie, inserted by a Set-Cookie directive from a server, belong to the same persistence session. * SSLSESSION - Connections that have the same SSL Session ID belong to the same persistence session. Possible values = SOURCEIP, COOKIEINSERT, SSLSESSION, NONE
persistmask	<String>	Read-write	Persistence mask for IP based persistence types, for IPv4 virtual servers. Minimum length = 1
v6persistmasklen	<Integer>	Read-write	Persistence mask for IP based persistence types, for IPv6 virtual servers. Default value: 128 Minimum value = 1 Maximum value = 128

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
timeout	<Integer>	Read-write	Time period for which a persistence session is in effect. Default value: 2 Minimum value = 0 Maximum value = 1440
cookiename	<String>	Read-write	Use this parameter to specify the cookie name for COOKIE peristence type. It specifies the name of cookie with a maximum of 32 characters. If not specified, cookie name is internally generated.
persistencebackup	<String>	Read-write	Backup persistence type for the virtual server. Becomes operational if the primary persistence mechanism fails. Possible values = SOURCEIP, NONE
backuppersistencetimeout	<Integer>	Read-write	Time period for which backup persistence is in effect. Default value: 2 Minimum value = 2

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum value = 1440
tcpprobeport	<Integer>	Read-write	Port number for external TCP probe. NetScaler provides support for external TCP health check of the vserver status over the selected port. This option is only supported for vservers assigned with an IPAddress or ipset. Minimum value = 1 Range 1 - 65535 * in CLI is represented as 65535 in NITRO API
probeprotocol	<String>	Read-write	Citrix ADC provides support for external health check of the vserver status. Select HTTP or TCP probes for healthcheck. Possible values = TCP, HTTP
probesuccessresponsecode	<String>	Read-write	HTTP code to return in SUCCESS case. Default value: "200 OK"

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum length = 1 Maximum length = 64
probeport	<Integer>	Read-write	Citrix ADC provides support for external health check of the vserver status. Select port for HTTP/ TCP monitring. Default value: 0 Range 1 - 65535 * in CLI is represented as 65535 in NITRO API
quicprofilename	<String>	Read-write	Name of QUIC profile which will be attached to the Content Switching VServer. Minimum length = 1 Maximum length = 255
redirectfromport	<Integer>	Read-write	Port number for the virtual server, from which we absorb the traffic for http redirect. Minimum value = 1 Range 1 - 65535 * in CLI is represented as

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			65535 in NITRO API
mcpprofilename	<String>	Read-write	Name of the MCP profile to attach to this cs vserver. Enables MCP protocol processing.
dnsoverhttps	<String>	Read-write	This option is used to enable/disable DNS over HTTPS (DoH) processing. Default value: DISABLED Possible values = ENABLED, DISABLED
httpsredirecturl	<String>	Read-write	URL to which all HTTP traffic received on the port specified in the -redirectFromPort parameter is redirected.
apiprofile	<String>	Read-write	The API profile where one or more API specs are bounded to. Minimum length = 1
wasmmodule	<String>	Read-write	Name of the WASM module to assign to this virtual server.
aigwprofilename	<String>	Read-write	Name of the AIGW frontend profile. For the content switching

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			vserver to function as AI gateway, this parameter must be set. Once this parameter is set using add cs vserver, it cannot be unset. Minimum length = 1 Maximum length = 255
domainname	<String>	Read-write	Domain name for which to change the time to live (TTL) and/or backup service IP address. Minimum length = 1
ttl	<Integer>	Read-write	. Minimum value = 1
backupip	<String>	Read-write	. Minimum length = 1
cookiedomain	<String>	Read-write	. Minimum length = 1
cookietimeout	<Integer>	Read-write	. Minimum value = 0 Maximum value = 1440
sitedomainttl	<Integer>	Read-write	. Minimum value = 1
newname	<String>	Read-write	New name for the virtual server. Must begin with an ASCII alphanumeric or

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at sign (@), equal sign (=), and hyphen (-) characters. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my name" or 'my name'). Minimum length = 1
ip	<String>	Read-only	The IP address of the virtual server.
value	<String>	Read-only	The ssl card status for the transparent ssl cs vserver. Possible values = Certkey/ Certkeybundle/Vault not bound/Cert-store not usable, SSL feature disabled

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ngname	<String>	Read-only	Nodegroup devno to which this csvserver belongs to.
type	<String>	Read-only	Virtual server type. Possible values = CONTENT, ADDRESS
curstate	<String>	Read-only	The state of the cs vserver. Possible values = UP, DOWN, UNKNOWN, BUSY, OUT OF SERVICE, GOING OUT OF SERVICE, DOWN WHEN GOING OUT OF SERVICE, NS_EMPTY_STR, Unknown, DISABLED
status	<Integer>	Read-only	Status.
cachetype	<String>	Read-only	Cache type. Possible values = TRANSPARENT, REVERSE, FORWARD
redirect	<String>	Read-only	Redirect URL string. Possible values = CACHE, POLICY, ORIGIN
homepage	<String>	Read-only	Home page.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
dnsvservername	<String>	Read-only	DNS vserver name.
domain	<String>	Read-only	Domain.
servicename	<String>	Read-only	Service name.
weight	<Integer>	Read-only	Weight for this service.
cachevserver	<String>	Read-only	Cache vserver name.
targetvserver	<String>	Read-only	target vserver name.
url	<String>	Read-only	URL string.
bindpoint	<String>	Read-only	The bindpoint to which the policy is bound. Possible values = REQUEST, RESPONSE, ICA_REQUEST, OTHERTCP_REQUEST, MQTT_JUMBO_REQ
gt2gb	<String>	Read-only	This argument has no effect. Default value: DISABLED Possible values = ENABLED, DISABLED
statechangetimesec	<String>	Read-only	Time when last state change happened. Seconds part.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
statechangetimemsec	<Integer>	Read-only	Time at which last state change happened. Milliseconds part.
tickssincelaststatechange	<Integer>	Read-only	Time in 10 millisecond ticks since the last state change.
ruletype	<Integer>	Read-only	Rule type.
lbvserver	<String>	Read-only	Name of the default lb vserver bound. Use this param for Default binding only. For Example: bind cs vserver cs1 -lbvserver lb1. Minimum length = 1
targetlbvserver	<String>	Read-only	target vserver name.
nodefaultbindings	<String>	Read-only	to determine if the configuration will have default ssl CIPHER and ECC curve bindings. Default value: NO Possible values = YES, NO
version	<Integer>	Read-only	Cookie version.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- ENABLE
- DISABLE
- GET (ALL)
- GET
- COUNT
- RENAME

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"csvserver":{

<b>"name":<String_value>,

</b>"td":<Integer_value>,

<b>"servicetype":<String_value>,

</b>"ipv46":<String_value>,

"targettype":<String_value>,

"dnsrecordtype":<String_value>,

"persistenceid":<Integer_value>,

"ippattern":<String_value>,

"ipmask":<String_value>,

"range":<Integer_value>,

"port":<Integer_value>,

"ipset":<String_value>,

"state":<String_value>,

"stateupdate":<String_value>,

"cacheable":<String_value>,
```

```
"redirecturl":<String_value>,

"clttimeout":<Integer_value>,

"precedence":<String_value>,

"casesensitive":<String_value>,

"somethod":<String_value>,

"sopersistence":<String_value>,

"sopersistencetimeout":<Integer_value>,

"sothreshold":<Integer_value>,

"sobackupaction":<String_value>,

"redirectportrewrite":<String_value>,

"downstateflush":<String_value>,

"backupvserver":<String_value>,

"disableprimaryondown":<String_value>,

"insertvserveripport":<String_value>,

"vipheader":<String_value>,

"rtspnat":<String_value>,

"authenticationhost":<String_value>,

"authentication":<String_value>,

"listenpolicy":<String_value>,

"listenpriority":<Integer_value>,

"authn401":<String_value>,

"authnvsname":<String_value>,
```

```
"push":<String_value>,

"pushvserver":<String_value>,

"pushlabel":<String_value>,

"pushmulticlients":<String_value>,

"tcpprofilename":<String_value>,

"httpprofilename":<String_value>,

"dbprofilename":<String_value>,

"oracleserverversion":<String_value>,

"comment":<String_value>,

"mssqlserverversion":<String_value>,

"l2conn":<String_value>,

"mysqlprotocolversion":<Integer_value>,

"mysqlserverversion":<String_value>,

"mysqlcharacterset":<Integer_value>,

"mysqlservercapabilities":<Integer_value>,

"appflowlog":<String_value>,

"netprofile":<String_value>,

"icmpvsrresponse":<String_value>,

"rhistate":<String_value>,

"authnprofile":<String_value>,

"dnsprofilename":<String_value>,

"dtls":<String_value>,
```

```
"persistencetype":<String_value>,

"persistmask":<String_value>,

"v6persistmasklen":<Integer_value>,

"timeout":<Integer_value>,

"cookiename":<String_value>,

"persistencebackup":<String_value>,

"backuppersistencetimeout":<Integer_value>,

"tcpprobeport":<Integer_value>,

"probeprotocol":<String_value>,

"probesuccessresponsecode":<String_value>,

"probeport":<Integer_value>,

"quicprofilename":<String_value>,

"redirectfromport":<Integer_value>,

"mcpprofilename":<String_value>,

"dnsoverhttps":<String_value>,

"httpsredirecturl":<String_value>,

"apiprofile":<String_value>,

"wasmmodule":<String_value>,

"aigwprofilename":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"csvserver":{

<b>"name":<String_value>,

</b>"ipv46":<String_value>,

"ipset":<String_value>,

"ippattern":<String_value>,

"ipmask":<String_value>,

"stateupdate":<String_value>,

"precedence":<String_value>,

"casesensitive":<String_value>,
```

```
"backupvserver":<String_value>,

"redirecturl":<String_value>,

"cacheable":<String_value>,

"clttimeout":<Integer_value>,

"somethod":<String_value>,

"sopersistence":<String_value>,

"sopersistencetimeout":<Integer_value>,

"sothreshold":<Integer_value>,

"sobackupaction":<String_value>,

"redirectportrewrite":<String_value>,

"downstateflush":<String_value>,

"disableprimaryondown":<String_value>,

"insertvserveripport":<String_value>,

"vipheader":<String_value>,

"rtspnat":<String_value>,

"authenticationhost":<String_value>,

"authentication":<String_value>,

"listenpolicy":<String_value>,

"listenpriority":<Integer_value>,

"authn401":<String_value>,

"authnvsname":<String_value>,

"push":<String_value>,
```

```
"pushvserver":<String_value>,

"pushlabel":<String_value>,

"pushmulticlients":<String_value>,

"tcpprofilename":<String_value>,

"httpprofilename":<String_value>,

"dbprofilename":<String_value>,

"mcpprofilename":<String_value>,

"comment":<String_value>,

"l2conn":<String_value>,

"mssqlserverversion":<String_value>,

"mysqlprotocolversion":<Integer_value>,

"oracleserverversion":<String_value>,

"mysqlserverversion":<String_value>,

"mysqlcharacterset":<Integer_value>,

"mysqlservercapabilities":<Integer_value>,

"appflowlog":<String_value>,

"netprofile":<String_value>,

"authnprofile":<String_value>,

"icmpvsrresponse":<String_value>,

"rhistate":<String_value>,

"dnsprofilename":<String_value>,

"dnsrecordtype":<String_value>,
```

```
"persistenceid":<Integer_value>,

"domainname":<String_value>,

"ttl":<Integer_value>,

"backupip":<String_value>,

"cookiedomain":<String_value>,

"cookietimeout":<Integer_value>,

"sitedomainttl":<Integer_value>,

"dtls":<String_value>,

"persistencetype":<String_value>,

"persistmask":<String_value>,

"v6persistmasklen":<Integer_value>,

"timeout":<Integer_value>,

"cookiename":<String_value>,

"persistencebackup":<String_value>,

"backuppersistencetimeout":<Integer_value>,

"tcpprobeport":<Integer_value>,

"probeprotocol":<String_value>,

"probesuccessresponsecode":<String_value>,

"probeport":<Integer_value>,

"quicprofilename":<String_value>,

"redirectfromport":<Integer_value>,

"httpsredirecturl":<String_value>,
```

```
"dnsoverhttps":<String_value>,

"apiprofile":<String_value>,

"wasmmodule":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"csvserver":{

<b>"name":<String_value>,

</b>"casesensitive":true,

"backupvserver":true,

"clttimeout":true,

"redirecturl":true,

"authn401":true,

"authentication":true,
```

```
"authenticationhost":true,

"authnvsname":true,

"pushvserver":true,

"pushlabel":true,

"tcpprofilename":true,

"httpprofilename":true,

"dbprofilename":true,

"l2conn":true,

"mysqlprotocolversion":true,

"mysqlserverversion":true,

"mysqlcharacterset":true,

"mysqlservercapabilities":true,

"appflowlog":true,

"netprofile":true,

"icmpvsrresponse":true,

"authnprofile":true,

"sothreshold":true,

"dnsprofilename":true,

"tcpprobeport":true,

"probeprotocol":true,

"quicprofilename":true,

"redirectfromport":true,
```

```
"httpsredirecturl":true,

"apiprofile":true,

"dnsoverhttps":true,

"wasmmodule":true,

"ipset":true,

"stateupdate":true,

"precedence":true,

"cacheable":true,

"somethod":true,

"sopersistence":true,

"sopersistencetimeout":true,

"sobackupaction":true,

"redirectportrewrite":true,

"downstateflush":true,

"disableprimaryondown":true,

"insertvserveripport":true,

"vipheader":true,

"rtspnat":true,

"listenpolicy":true,

"listenpriority":true,

"push":true,

"pushmulticlients":true,
```

```
"mcpprofilename":true,

"comment":true,

"mssqlserverversion":true,

"oracleserverversion":true,

"rhistate":true,

"dnsrecordtype":true,

"persistenceid":true,

"dtls":true,

"persistencetype":true,

"persistmask":true,

"v6persistmasklen":true,

"timeout":true,

"cookiename":true,

"persistencebackup":true,

"backuppersistencetimeout":true,

"probesuccessresponsecode":true

}}
```


Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

ENABLE

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver? **action=enable HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"csvserver":{

<b>"name":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DISABLE

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver? **action=disable HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"csvserver":{

<b>"name":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

RENAME

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver? **action=rename HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"csvserver":{

<b>"name":<String_value>,

</b><b>"newname":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/csvserver? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/csvserver? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of csvserver resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/csvserver? **view=summary**

Use this query-parameter to get the summary output of csvserver resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/csvserver? **pagesize=#no;pageno=#no**

Use this query-parameter to get the csvserver resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "csvserver": [ {

"name":<String_value>,

"insertvserveripport":<String_value>,

"vipheader":<String_value>,

"ip":<String_value>,

"td":<Integer_value>,

"ipv46":<String_value>,

"ippattern":<String_value>,
```

```
"ipmask":<String_value>,

"value":<String_value>,

"port":<Integer_value>,

"ipset":<String_value>,

"range":<Integer_value>,

"servicetype":<String_value>,

"ngname":<String_value>,

"type":<String_value>,

"curstate":<String_value>,

"stateupdate":<String_value>,

"status":<Integer_value>,

"cachetype":<String_value>,

"redirect":<String_value>,

"precedence":<String_value>,

"redirecturl":<String_value>,

"authentication":<String_value>,

"authn401":<String_value>,

"authnvsname":<String_value>,

"casesensitive":<String_value>,

"homepage":<String_value>,

"dnsvservername":<String_value>,

"domain":<String_value>,
```

```
"servicename":<String_value>,

"weight":<Integer_value>,

"cachevserver":<String_value>,

"targetvserver":<String_value>,

"backupvserver":<String_value>,

"clttimeout":<Integer_value>,

"listenpolicy":<String_value>,

"listenpriority":<Integer_value>,

"somethod":<String_value>,

"sopersistence":<String_value>,

"sopersistencetimeout":<Integer_value>,

"sothreshold":<Integer_value>,

"sobackupaction":<String_value>,

"cacheable":<String_value>,

"url":<String_value>,

"redirectportrewrite":<String_value>,

"downstateflush":<String_value>,

"disableprimaryondown":<String_value>,

"bindpoint":<String_value>,

"gt2gb":<String_value>,

"statechangetimesec":<String_value>,

"statechangetimemsec":<Integer_value>,
```

```
"tickssincelaststatechange":<Integer_value>,

"rtspnat":<String_value>,

"authenticationhost":<String_value>,

"push":<String_value>,

"pushvserver":<String_value>,

"pushlabel":<String_value>,

"pushmulticlients":<String_value>,

"tcpprofilename":<String_value>,

"httpprofilename":<String_value>,

"dbprofilename":<String_value>,

"comment":<String_value>,

"oracleserverversion":<String_value>,

"mssqlserverversion":<String_value>,

"l2conn":<String_value>,

"ruletype":<Integer_value>,

"mysqlprotocolversion":<Integer_value>,

"mysqlserverversion":<String_value>,

"mysqlcharacterset":<Integer_value>,

"mysqlservercapabilities":<Integer_value>,

"appflowlog":<String_value>,

"netprofile":<String_value>,

"icmpvsrresponse":<String_value>,
```

```
"rhistate":<String_value>,

"lbvserver":<String_value>,

"targetlbvserver":<String_value>,

"authnprofile":<String_value>,

"dnsprofilename":<String_value>,

"targettype":<String_value>,

"domainname":<String_value>,

"ttl":<Integer_value>,

"backupip":<String_value>,

"cookiedomain":<String_value>,

"cookietimeout":<Integer_value>,

"sitedomainttl":<Integer_value>,

"dnsrecordtype":<String_value>,

"persistenceid":<Integer_value>,

"dtls":<String_value>,

"nodefaultbindings":<String_value>,

"persistencetype":<String_value>,

"persistmask":<String_value>,

"v6persistmasklen":<Integer_value>,

"timeout":<Integer_value>,

"cookiename":<String_value>,

"version":<Integer_value>,
```

```
"persistencebackup":<String_value>,

"backuppersistencetimeout":<Integer_value>,

"tcpprobeport":<Integer_value>,

"probeprotocol":<String_value>,

"probeport":<Integer_value>,

"probesuccessresponsecode":<String_value>,

"quicprofilename":<String_value>,

"redirectfromport":<Integer_value>,

"httpsredirecturl":<String_value>,

"apiprofile":<String_value>,

"mcpprofilename":<String_value>,

"dnsoverhttps":<String_value>,

"wasmmodule":<String_value>,

"aigwprofilename":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/csvserver/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/csvserver/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of csvserver resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "csvserver": [ {

"name":<String_value>,

"insertvserveripport":<String_value>,

"vipheader":<String_value>,

"ip":<String_value>,

"td":<Integer_value>,

"ipv46":<String_value>,

"ippattern":<String_value>,

"ipmask":<String_value>,

"value":<String_value>,
```

```
"port":<Integer_value>,

"ipset":<String_value>,

"range":<Integer_value>,

"servicetype":<String_value>,

"ngname":<String_value>,

"type":<String_value>,

"curstate":<String_value>,

"stateupdate":<String_value>,

"status":<Integer_value>,

"cachetype":<String_value>,

"redirect":<String_value>,

"precedence":<String_value>,

"redirecturl":<String_value>,

"authentication":<String_value>,

"authn401":<String_value>,

"authnvsname":<String_value>,

"casesensitive":<String_value>,

"homepage":<String_value>,

"dnsvservername":<String_value>,

"domain":<String_value>,

"servicename":<String_value>,

"weight":<Integer_value>,
```

```
"cachevserver":<String_value>,

"targetvserver":<String_value>,

"backupvserver":<String_value>,

"clttimeout":<Integer_value>,

"listenpolicy":<String_value>,

"listenpriority":<Integer_value>,

"somethod":<String_value>,

"sopersistence":<String_value>,

"sopersistencetimeout":<Integer_value>,

"sothreshold":<Integer_value>,

"sobackupaction":<String_value>,

"cacheable":<String_value>,

"url":<String_value>,

"redirectportrewrite":<String_value>,

"downstateflush":<String_value>,

"disableprimaryondown":<String_value>,

"bindpoint":<String_value>,

"gt2gb":<String_value>,

"statechangetimesec":<String_value>,

"statechangetimemsec":<Integer_value>,

"tickssincelaststatechange":<Integer_value>,

"rtspnat":<String_value>,
```

```
"authenticationhost":<String_value>,

"push":<String_value>,

"pushvserver":<String_value>,

"pushlabel":<String_value>,

"pushmulticlients":<String_value>,

"tcpprofilename":<String_value>,

"httpprofilename":<String_value>,

"dbprofilename":<String_value>,

"comment":<String_value>,

"oracleserverversion":<String_value>,

"mssqlserverversion":<String_value>,

"l2conn":<String_value>,

"ruletype":<Integer_value>,

"mysqlprotocolversion":<Integer_value>,

"mysqlserverversion":<String_value>,

"mysqlcharacterset":<Integer_value>,

"mysqlservercapabilities":<Integer_value>,

"appflowlog":<String_value>,

"netprofile":<String_value>,

"icmpvsrresponse":<String_value>,

"rhistate":<String_value>,

"lbvserver":<String_value>,
```

```
"targetlbvserver":<String_value>,

"authnprofile":<String_value>,

"dnsprofilename":<String_value>,

"targettype":<String_value>,

"domainname":<String_value>,

"ttl":<Integer_value>,

"backupip":<String_value>,

"cookiedomain":<String_value>,

"cookietimeout":<Integer_value>,

"sitedomainttl":<Integer_value>,

"dnsrecordtype":<String_value>,

"persistenceid":<Integer_value>,

"dtls":<String_value>,

"nodefaultbindings":<String_value>,

"persistencetype":<String_value>,

"persistmask":<String_value>,

"v6persistmasklen":<Integer_value>,

"timeout":<Integer_value>,

"cookiename":<String_value>,

"version":<Integer_value>,

"persistencebackup":<String_value>,

"backuppersistencetimeout":<Integer_value>,
```

```
"tcpprobeport":<Integer_value>,

"probeprotocol":<String_value>,

"probeport":<Integer_value>,

"probesuccessresponsecode":<String_value>,

"quicprofilename":<String_value>,

"redirectfromport":<Integer_value>,

"httpsredirecturl":<String_value>,

"apiprofile":<String_value>,

"mcpprofilename":<String_value>,

"dnsoverhttps":<String_value>,

"wasmmodule":<String_value>,

"aigwprofilename":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "csvserver": [ { "__count": "#no"} ] }
```

csvserver_analyticsprofile_binding

Binding object showing the analyticsprofile that can be bound to csvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the content switching virtual server to which the content switching policy applies. Minimum length = 1
analyticsprofile	<String>	Read-write	Name of the analytics profile bound to the LB vserver.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/csvserver_analyticsprofile_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"csvserver_analyticsprofile_binding":{
```

```
<b>"name":<String_value>,

</b>"analyticsprofile":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver_analyticsprofile_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ csvserver_analyticsprofile_binding/ name_value<String> ? **args=analyticsprofile: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver_analyticsprofile_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ csvserver_analyticsprofile_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of csvserver_analyticsprofile_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/csvserver_analyticsprofile_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the csvserver_analyticsprofile_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "csvserver_analyticsprofile_binding": [ {

"name":<String_value>,

"analyticsprofile":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver_analyticsprofile_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/csvserver_analyticsprofile_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "csvserver_analyticsprofile_binding": [ {

"name":<String_value>,

"analyticsprofile":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver_analyticsprofile_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"csvserver_analyticsprofile_binding": [ { "__count": "#no"} ] }
```

csvserver_appflowpolicy_binding

Binding object showing the appflowpolicy that can be bound to csvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
policyname	<String>	Read-write	Policies bound to this vserver.
invoke	<Boolean>	Read-write	Invoke flag.
gotopriorityexpression	<String>	Read-write	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
targetlbvserver	<String>	Read-write	Name of the Load Balancing virtual server to which the content is switched, if policy rule is evaluated to be TRUE. Example: bind cs vs cs1 -policyname pol1 -priority 101 -targetLBVserver lb1 Note: Use this parameter only in case of Content Switching policy bind operations to a CS vserver. Minimum length = 1
labelname	<String>	Read-write	Name of the label invoked.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
priority	<Integer>	Read-write	Priority for the policy.
labeltype	<String>	Read-write	The invocation type. Possible values = reqvserver, resvserver, policylabel
bindpoint	<String>	Read-write	Bind point at which policy needs to be bound. Note: Content switching policies are evaluated only at request time. Possible values = REQUEST, RESPONSE, ICA_REQUEST, OTHERTCP_REQUEST, MQTT_JUMBO_REQ
name	<String>	Read-write	Name of the content switching virtual server to which the content switching policy applies. Minimum length = 1
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/csvserver_appflowpolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"csvserver_appflowpolicy_binding":{

<b>"name":<String_value>,

</b>"policyname":<String_value>,

"targetlbvserver":<String_value>,

"priority":<Integer_value>,

"gotopriorityexpression":<String_value>,

"bindpoint":<String_value>,

"invoke":<Boolean_value>,

"labeltype":<String_value>,

"labelname":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver_appflowpolicy_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ csvserver_appflowpolicy_binding/ name_value<String> ? **args=policyname: <String_value> ,bindpoint: <String_value> ,priority: <Integer_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver_appflowpolicy_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ csvserver_appflowpolicy_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of csvserver_appflowpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/csvserver_appflowpolicy_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the csvserver_appflowpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "csvserver_appflowpolicy_binding": [ {

"policyname":<String_value>,

"invoke":<Boolean_value>,

"gotopriorityexpression":<String_value>,
```

```
"targetlbvserver":<String_value>,

"labelname":<String_value>,

"priority":<Integer_value>,

"labeltype":<String_value>,

"bindpoint":<String_value>,

"name":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver_appflowpolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/csvserver_appflowpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "csvserver_appflowpolicy_binding": [ {

"policyname":<String_value>,

"invoke":<Boolean_value>,

"gotopriorityexpression":<String_value>,

"targetlbvserver":<String_value>,

"labelname":<String_value>,

"priority":<Integer_value>,

"labeltype":<String_value>,

"bindpoint":<String_value>,

"name":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver_appflowpolicy_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"csvserver_appflowpolicy_binding": [ { "__count": "#no"} ] }
```

csvserver_appfwpolicy_binding

Binding object showing the appfwpolicy that can be bound to csvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
targetlbvserver	<String>	Read-write	Name of the Load Balancing virtual server to which the content is switched, if policy rule is evaluated to be TRUE. Example: bind cs vs cs1 -policyname pol1 -priority 101 -targetLBVserver lb1 Note: Use this parameter only in case of Content Switching policy bind operations to a CS vserver. Minimum length = 1
invoke	<Boolean>	Read-write	Invoke flag.
gotopriorityexpression	<String>	Read-write	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
policyname	<String>	Read-write	Policies bound to this vserver.
name	<String>	Read-write	Name of the content switching virtual server to which the content switching policy applies. Minimum length = 1
priority	<Integer>	Read-write	Priority for the policy.
labeltype	<String>	Read-write	The invocation type. Possible values = reqvserver, resvserver, policylabel
bindpoint	<String>	Read-write	The bindpoint to which the policy is bound. Possible values = REQUEST, RESPONSE, ICA_REQUEST, OTHERTCP_REQUEST, MQTT_JUMBO_REQ
labelname	<String>	Read-write	Name of the label invoked.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD

- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/csvserver_appfwpolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"csvserver_appfwpolicy_binding":{

<b>"name":<String_value>,

</b>"policyname":<String_value>,

"targetlbvserver":<String_value>,

"priority":<Integer_value>,

"gotopriorityexpression":<String_value>,

"bindpoint":<String_value>,

"invoke":<Boolean_value>,

"labeltype":<String_value>,

"labelname":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver_appfwpolicy_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ csvserver_appfwpolicy_binding/ name_value<String> ? **args=policyname: <String_value> ,bindpoint: <String_value> ,priority: <Integer_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver_appfwpolicy_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ csvserver_appfwpolicy_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of csvserver_appfwpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/csvserver_appfwpolicy_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the csvserver_appfwpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "csvserver_appfwpolicy_binding": [ {

"targetlbvserver":<String_value>,

"invoke":<Boolean_value>,
```

```
"gotopriorityexpression":<String_value>,

"policyname":<String_value>,

"name":<String_value>,

"priority":<Integer_value>,

"labeltype":<String_value>,

"bindpoint":<String_value>,

"labelname":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver_appfwpolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/csvserver_appfwpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "csvserver_appfwpolicy_binding": [ {

"targetlbvserver":<String_value>,

"invoke":<Boolean_value>,

"gotopriorityexpression":<String_value>,

"policyname":<String_value>,

"name":<String_value>,

"priority":<Integer_value>,

"labeltype":<String_value>,

"bindpoint":<String_value>,

"labelname":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver_appfwpolicy_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"csvserver_appfwpolicy_binding": [ { "__count": "#no"} ] }
```

csvserver_appqoepolicy_binding

Binding object showing the appqoepolicy that can be bound to csvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
targetlbvserver	<String>	Read-write	Name of the Load Balancing virtual server to which the content is switched, if policy rule is evaluated to be TRUE. Example: bind cs vs cs1 -policyname pol1 -priority 101 -targetLBVserver lb1 Note: Use this parameter only in case of Content Switching policy bind operations to a CS vserver. Minimum length = 1
policyname	<String>	Read-write	Policies bound to this vserver.
invoke	<Boolean>	Read-write	Invoke flag.
gotopriorityexpression	<String>	Read-write	Expression specifying the priority of the next policy which will get

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			evaluated if the current policy rule evaluates to TRUE.
priority	<Integer>	Read-write	Priority for the policy.
labeltype	<String>	Read-write	The invocation type. Possible values = reqvserver, resvserver, policylabel
bindpoint	<String>	Read-write	The bindpoint to which the policy is bound. Possible values = REQUEST, RESPONSE, ICA_REQUEST, OTHERTCP_REQUEST, MQTT_JUMBO_REQ
name	<String>	Read-write	Name of the content switching virtual server to which the content switching policy applies. Minimum length = 1
labelname	<String>	Read-write	Name of the label invoked.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/csvserver_appqoepolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"csvserver_appqoepolicy_binding":{

<b>"name":<String_value>,

</b>"policyname":<String_value>,

"targetlbvserver":<String_value>,

"priority":<Integer_value>,

"gotopriorityexpression":<String_value>,

"bindpoint":<String_value>,

"invoke":<Boolean_value>,

"labeltype":<String_value>,

"labelname":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver_appqoepolicy_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ csvserver_appqoepolicy_binding/ name_value<String> ? **args=policyname: <String_value> ,bindpoint: <String_value> ,priority: <Integer_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver_appqoepolicy_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ csvserver_appqoepolicy_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of csvserver_appqoepolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/csvserver_appqoepolicy_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the csvserver_appqoepolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "csvserver_appqoepolicy_binding": [ {

"targetlbvserver":<String_value>,
```

```
"policyname":<String_value>,

"invoke":<Boolean_value>,

"gotopriorityexpression":<String_value>,

"priority":<Integer_value>,

"labeltype":<String_value>,

"bindpoint":<String_value>,

"name":<String_value>,

"labelname":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver_appqoepolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/csvserver_appqoepolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "csvserver_appqoepolicy_binding": [ {

"targetlbvserver":<String_value>,

"policyname":<String_value>,

"invoke":<Boolean_value>,

"gotopriorityexpression":<String_value>,

"priority":<Integer_value>,

"labeltype":<String_value>,

"bindpoint":<String_value>,

"name":<String_value>,

"labelname":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver_appqoepolicy_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"csvserver_appqoepolicy_binding": [ { "__count": "#no"} ] }
```

csvserver_auditnslogpolicy_binding

Binding object showing the auditnslogpolicy that can be bound to csvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
gotopriorityexpression	<String>	Read-write	Expression or other value specifying the next policy to be evaluated if the current policy evaluates to TRUE. Specify one of the following values: * NEXT - Evaluate the policy with the next higher priority number. * END - End policy evaluation. * USE_INVOCATION_RESULT - Applicable if this policy invokes another policy label. If the final goto in the invoked policy label has a value of END, the evaluation stops. If the final goto is anything other than END, the current policy label performs a NEXT. * An

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			expression that evaluates to a number. If you specify an expression, the number to which it evaluates determines the next policy to evaluate, as follows: * If the expression evaluates to a higher numbered priority, the policy with that priority is evaluated next. * If the expression evaluates to the priority of the current policy, the policy with the next higher numbered priority is evaluated next. * If the expression evaluates to a priority number that is numerically higher than the highest numbered priority, policy evaluation ends. An UNDEF event is triggered if: * The expression is invalid. * The expression evaluates to a priority number that is numerically lower than the current policy's priority. * The expression evaluates to a priority number

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			that is between the current policy's priority number (say, 30) and the highest priority number (say, 100), but does not match any configured priority number (for example, the expression evaluates to the number 85). This example assumes that the priority number increments by 10 for every successive policy, and therefore a priority number of 85 does not exist in the policy label.
invoke	<Boolean>	Read-write	Invoke a policy label if this policy's rule evaluates to TRUE.
policyname	<String>	Read-write	Policies bound to this vserver.
targetlbvserver	<String>	Read-write	Name of the Load Balancing virtual server to which the content is switched, if policy rule is evaluated to be TRUE. Example: bind cs vs cs1 -policyname pol1 -priority 101 -targetLBVserver lb1 Note: Use this

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			parameter only in case of Content Switching policy bind operations to a CS vserver. Minimum length = 1
labelname	<String>	Read-write	Name of the label to be invoked.
name	<String>	Read-write	Name of the content switching virtual server to which the content switching policy applies. Minimum length = 1
bindpoint	<String>	Read-write	Bind point at which policy needs to be bound. Note: Content switching policies are evaluated only at request time. Possible values = REQUEST, RESPONSE, ICA_REQUEST, OTHERTCP_REQUEST, MQTT_JUMBO_REQ
labeltype	<String>	Read-write	Type of label to be invoked. Possible values = reqvserver, resvserver, policylabel

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
priority	<Integer>	Read-write	Priority for the policy.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/csvserver_auditnslogpolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"csvserver_auditnslogpolicy_binding":{

<b>"name":<String_value>,

</b>"policyname":<String_value>,

"targetlbvserver":<String_value>,

"priority":<Integer_value>,

"gotopriorityexpression":<String_value>,

"bindpoint":<String_value>,

"invoke":<Boolean_value>,

"labeltype":<String_value>,

"labelname":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver_auditnslogpolicy_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ csvserver_auditnslogpolicy_binding/ name_value<String> ? **args=policyname: <String_value> ,bindpoint: <String_value> ,priority: <Integer_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver_auditnslogpolicy_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ csvserver_auditnslogpolicy_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of csvserver_auditnslogpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/csvserver_auditnslogpolicy_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the csvserver_auditnslogpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "csvserver_auditnslogpolicy_binding": [ {

"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>,

"policyname":<String_value>,

"targetlbvserver":<String_value>,

"labelname":<String_value>,

"name":<String_value>,

"bindpoint":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver_auditnslogpolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/csvserver_auditnslogpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "csvserver_auditnslogpolicy_binding": [ {

"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>,

"policyname":<String_value>,

"targetlbvserver":<String_value>,

"labelname":<String_value>,

"name":<String_value>,

"bindpoint":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver_auditnslogpolicy_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"csvserver_auditnslogpolicy_binding": [ { "__count": "#no"} ] }
```

csvserver_auditsyslogpolicy_binding

Binding object showing the auditsyslogpolicy that can be bound to csvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
labelname	<String>	Read-write	Name of the label to be invoked.
name	<String>	Read-write	Name of the content switching virtual server to which the content switching policy applies. Minimum length = 1
priority	<Integer>	Read-write	Priority for the policy.
labeltype	<String>	Read-write	Type of label to be invoked. Possible values = reqvserver,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			resvserver, policylabel
bindpoint	<String>	Read-write	Bind point at which policy needs to be bound. Note: Content switching policies are evaluated only at request time. Possible values = REQUEST, RESPONSE, ICA_REQUEST, OTHERTCP_REQUEST, MQTT_JUMBO_REQ
invoke	<Boolean>	Read-write	Invoke a policy label if this policy's rule evaluates to TRUE.
gotopriorityexpression	<String>	Read-write	Expression or other value specifying the next policy to be evaluated if the current policy evaluates to TRUE. Specify one of the following values: * NEXT - Evaluate the policy with the next higher priority number. * END - End policy evaluation. * USE_INVOCATION_RESULT - Applicable if this policy invokes another policy label.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			If the final goto in the invoked policy label has a value of END, the evaluation stops. If the final goto is anything other than END, the current policy label performs a NEXT. * An expression that evaluates to a number. If you specify an expression, the number to which it evaluates determines the next policy to evaluate, as follows: * If the expression evaluates to a higher numbered priority, the policy with that priority is evaluated next. * If the expression evaluates to the priority of the current policy, the policy with the next higher numbered priority is evaluated next. * If the expression evaluates to a priority number that is numerically higher than the highest numbered priority, policy evaluation ends. An UNDEF event is triggered if: * The

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			expression is invalid. * The expression evaluates to a priority number that is numerically lower than the current policy's priority. * The expression evaluates to a priority number that is between the current policy's priority number (say, 30) and the highest priority number (say, 100), but does not match any configured priority number (for example, the expression evaluates to the number 85). This example assumes that the priority number increments by 10 for every successive policy, and therefore a priority number of 85 does not exist in the policy label.
policyname	<String>	Read-write	Policies bound to this vserver.
targetlbvserver	<String>	Read-write	Name of the Load Balancing virtual server to which the content is switched, if policy rule is evaluated to be TRUE. Example:

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			bind cs vs cs1 -policyname pol1 -priority 101 -targetLBVserver lb1 Note: Use this parameter only in case of Content Switching policy bind operations to a CS vserver. Minimum length = 1
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/csvserver_auditsyslogpolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"csvserver_auditsyslogpolicy_binding":{

<b>"name":<String_value>,

</b>"policyname":<String_value>,

"targetlbvserver":<String_value>,

"priority":<Integer_value>,

"gotopriorityexpression":<String_value>,

"bindpoint":<String_value>,

"invoke":<Boolean_value>,

"labeltype":<String_value>,
```

```
"labelname":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver_auditsyslogpolicy_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ csvserver_auditsyslogpolicy_binding/ name_value<String> ? **args=policyname: <String_value> ,bindpoint: <String_value> ,priority: <Integer_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver_auditsyslogpolicy_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ csvserver_auditsyslogpolicy_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of csvserver_auditsyslogpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/csvserver_auditsyslogpolicy_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the csvserver_auditsyslogpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "csvserver_auditsyslogpolicy_binding": [ {

"labelname":<String_value>,

"name":<String_value>,

"priority":<Integer_value>,

"labeltype":<String_value>,

"bindpoint":<String_value>,

"invoke":<Boolean_value>,

"gotopriorityexpression":<String_value>,

"policyname":<String_value>,

"targetlbvserver":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver_auditsyslogpolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ csvserver_auditsyslogpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "csvserver_auditsyslogpolicy_binding": [ {

"labelname":<String_value>,

"name":<String_value>,

"priority":<Integer_value>,

"labeltype":<String_value>,

"bindpoint":<String_value>,

"invoke":<Boolean_value>,

"gotopriorityexpression":<String_value>,

"policyname":<String_value>,

"targetlbvserver":<String_value>
```

```
}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver_auditsyslogpolicy_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"csvserver_auditsyslogpolicy_binding": [ { "__count": "#no"} ] }
```

csvserver_authorizationpolicy_binding

Binding object showing the authorizationpolicy that can be bound to csvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
priority	<Integer>	Read-write	Priority for the policy.
labeltype	<String>	Read-write	The invocation type. Possible values = reqvserver,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			resvserver, policylabel
bindpoint	<String>	Read-write	The bindpoint to which the policy is bound. Possible values = REQUEST, RESPONSE, ICA_REQUEST, OTHERTCP_REQUEST, MQTT_JUMBO_REQ
name	<String>	Read-write	Name of the content switching virtual server to which the content switching policy applies. Minimum length = 1
labelname	<String>	Read-write	Name of the label invoked.
targetlbvserver	<String>	Read-write	Name of the Load Balancing virtual server to which the content is switched, if policy rule is evaluated to be TRUE. Example: bind cs vs cs1 -policyname pol1 -priority 101 -targetLBVserver lb1 Note: Use this parameter only in case of Content Switching policy bind

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			operations to a CS vserver. Minimum length = 1
policyname	<String>	Read-write	Policies bound to this vserver.
invoke	<Boolean>	Read-write	Invoke flag.
gotopriorityexpression	<String>	Read-write	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/csvserver_authorizationpolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"csvserver_authorizationpolicy_binding":{

<b>"name":<String_value>,

</b>"policyname":<String_value>,

"targetlbvserver":<String_value>,

"priority":<Integer_value>,

"gotopriorityexpression":<String_value>,
```

```
"bindpoint":<String_value>,

"invoke":<Boolean_value>,

"labeltype":<String_value>,

"labelname":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver_authorizationpolicy_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ csvserver_authorizationpolicy_binding/ name_value<String> ? **args=policyname: <String_value> ,bindpoint: <String_value> ,priority: <Integer_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver_authorizationpolicy_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ csvserver_authorizationpolicy_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of csvserver_authorizationpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/csvserver_authorizationpolicy_binding/name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the csvserver_authorizationpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "csvserver_authorizationpolicy_binding": [ {

"priority":<Integer_value>,

"labeltype":<String_value>,

"bindpoint":<String_value>,

"name":<String_value>,

"labelname":<String_value>,

"targetlbvserver":<String_value>,

"policyname":<String_value>,

"invoke":<Boolean_value>,

"gotopriorityexpression":<String_value>
```

```
}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver_authorizationpolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/csvserver_authorizationpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "csvserver_authorizationpolicy_binding": [ {

"priority":<Integer_value>,

"labeltype":<String_value>,

"bindpoint":<String_value>,

"name":<String_value>,

"labelname":<String_value>,
```

```
"targetlbvserver":<String_value>,

"policyname":<String_value>,

"invoke":<Boolean_value>,

"gotopriorityexpression":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver_authorizationpolicy_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"csvserver_authorizationpolicy_binding": [ { "__count": "#no"} ] }
```

csvserver_binding

Binding object which returns the resources bound to csvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of a content switching virtual server for which to display information, including the policies bound to the virtual server. To display a list of all configured Content Switching virtual servers, do not specify a value for this parameter. Minimum length = 1
csvserver_transformpolicy_binding	<csvserver_transformpolicy_binding[]>	Read-only	transformpolicy that can be bound to csvserver.
csvserver_domain_binding	<csvserver_domain_binding[]>	Read-only	domain that can be bound to csvserver.
csvserver_spilloverpolicy_binding	<csvserver_spilloverpolicy_binding[]>	Read-only	spilloverpolicy that can be bound to csvserver.
csvserver_rewritepolicy_binding	<csvserver_rewritepolicy_binding[]>	Read-only	rewritepolicy that can be bound to csvserver.
csvserver_feopolicy_binding	<csvserver_feopolicy_binding[]>	Read-only	feopolicy that can be bound to csvserver.
csvserver_cachepolicy_binding	<csvserver_cachepolicy_binding[]>	Read-only	cachepolicy that can be bound to csvserver.
csvserver_cmppolicy_binding	<csvserver_cmppolicy_binding[]>	Read-only	cmppolicy that can be bound to csvserver.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
csvserver_lbvserver_binding	<csvserver_lbvserver_binding[]>	Read-only	lbvserver that can be bound to csvserver.
csvserver_auditsyslogpolicy_binding	<csvserver_auditsyslogpolicy_binding[]>	Read-only	auditsyslogpolicy that can be bound to csvserver.
csvserver_cspolicy_binding	<csvserver_cspolicy_binding[]>	Read-only	cspolicy that can be bound to csvserver.
csvserver_contentinspectionpolicy_binding	<csvserver_contentinspectionpolicy_binding[]>	Read-only	contentinspectionpolicy that can be bound to csvserver.
csvserver_appfwpolicy_binding	<csvserver_appfwpolicy_binding[]>	Read-only	appfwpolicy that can be bound to csvserver.
csvserver_responderpolicy_binding	<csvserver_responderpolicy_binding[]>	Read-only	responderpolicy that can be bound to csvserver.
csvserver_vpnvserver_binding	<csvserver_vpnvserver_binding[]>	Read-only	vpnvserver that can be bound to csvserver.
csvserver_appqoepolicy_binding	<csvserver_appqoepolicy_binding[]>	Read-only	appqoepolicy that can be bound to csvserver.
csvserver_auditnslogpolicy_binding	<csvserver_auditnslogpolicy_binding[]>	Read-only	auditnslogpolicy that can be bound to csvserver.
csvserver_botpolicy_binding	<csvserver_botpolicy_binding[]>	Read-only	botpolicy that can be bound to csvserver.
csvserver_authorizationpolicy_binding	<csvserver_authorizationpolicy_binding[]>	Read-only	authorizationpolicy that can be bound to csvserver.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
csvserver_appflowpolicy_binding	<csvserver_appflowpolicy_binding[]>	Read-only	appflowpolicy that can be bound to csvserver.
csvserver_gslbvserver_binding	<csvserver_gslbvserver_binding[]>	Read-only	gslbvserver that can be bound to csvserver.
csvserver_tmtrafficpolicy_binding	<csvserver_tmtrafficpolicy_binding[]>	Read-only	tmtrafficpolicy that can be bound to csvserver.
csvserver_analyticsprofile_binding	<csvserver_analyticsprofile_binding[]>	Read-only	analyticsprofile that can be bound to csvserver.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver_binding/ name_value<String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "csvserver_binding": [ {

"name":<String_value>,

"csvserver_appqoepolicy_binding":<csvserver_appqoepolicy_binding[]_value>,

"csvserver_contentinspectionpolicy_binding":<csvserver_contentinspectionpo
licy_binding[]_value>,

"csvserver_cmppolicy_binding":<csvserver_cmppolicy_binding[]_value>,

"csvserver_feopolicy_binding":<csvserver_feopolicy_binding[]_value>,

"csvserver_rewritepolicy_binding":<csvserver_rewritepolicy_binding[]_value
```

```
>,

"csvserver_appfwpolicy_binding":<csvserver_appfwpolicy_binding[]_value>,

"csvserver_cachepolicy_binding":<csvserver_cachepolicy_binding[]_value>,

"csvserver_responderpolicy_binding":<csvserver_responderpolicy_binding[]_v
alue>,

"csvserver_vpnvserver_binding":<csvserver_vpnvserver_binding[]_value>,

"csvserver_spilloverpolicy_binding":<csvserver_spilloverpolicy_binding[]_v
alue>,

"csvserver_domain_binding":<csvserver_domain_binding[]_value>,

"csvserver_appflowpolicy_binding":<csvserver_appflowpolicy_binding[]_value
>,

"csvserver_analyticsprofile_binding":<csvserver_analyticsprofile_binding[]
_value>,

"csvserver_authorizationpolicy_binding":<csvserver_authorizationpolicy_bin
ding[]_value>,

"csvserver_botpolicy_binding":<csvserver_botpolicy_binding[]_value>,

"csvserver_lbvserver_binding":<csvserver_lbvserver_binding[]_value>,

"csvserver_gslbvserver_binding":<csvserver_gslbvserver_binding[]_value>,

"csvserver_transformpolicy_binding":<csvserver_transformpolicy_binding[]_v
alue>,

"csvserver_auditnslogpolicy_binding":<csvserver_auditnslogpolicy_binding[]
_value>,

"csvserver_auditsyslogpolicy_binding":<csvserver_auditsyslogpolicy_binding
[]_value>,

"csvserver_cspolicy_binding":<csvserver_cspolicy_binding[]_value>,

"csvserver_tmtrafficpolicy_binding":<csvserver_tmtrafficpolicy_binding[]_v
alue>
```

```
}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/csvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "csvserver_binding": [ {

"name":<String_value>,

"csvserver_appqoepolicy_binding":<csvserver_appqoepolicy_binding[]_value>,

"csvserver_contentinspectionpolicy_binding":<csvserver_contentinspectionpo
licy_binding[]_value>,

"csvserver_cmppolicy_binding":<csvserver_cmppolicy_binding[]_value>,

"csvserver_feopolicy_binding":<csvserver_feopolicy_binding[]_value>,
```

```
"csvserver_rewritepolicy_binding":<csvserver_rewritepolicy_binding[]_value
>,

"csvserver_appfwpolicy_binding":<csvserver_appfwpolicy_binding[]_value>,

"csvserver_cachepolicy_binding":<csvserver_cachepolicy_binding[]_value>,

"csvserver_responderpolicy_binding":<csvserver_responderpolicy_binding[]_v
alue>,

"csvserver_vpnvserver_binding":<csvserver_vpnvserver_binding[]_value>,

"csvserver_spilloverpolicy_binding":<csvserver_spilloverpolicy_binding[]_v
alue>,

"csvserver_domain_binding":<csvserver_domain_binding[]_value>,

"csvserver_appflowpolicy_binding":<csvserver_appflowpolicy_binding[]_value
>,

"csvserver_analyticsprofile_binding":<csvserver_analyticsprofile_binding[]
_value>,

"csvserver_authorizationpolicy_binding":<csvserver_authorizationpolicy_bin
ding[]_value>,

"csvserver_botpolicy_binding":<csvserver_botpolicy_binding[]_value>,

"csvserver_lbvserver_binding":<csvserver_lbvserver_binding[]_value>,

"csvserver_gslbvserver_binding":<csvserver_gslbvserver_binding[]_value>,

"csvserver_transformpolicy_binding":<csvserver_transformpolicy_binding[]_v
alue>,

"csvserver_auditnslogpolicy_binding":<csvserver_auditnslogpolicy_binding[]
_value>,

"csvserver_auditsyslogpolicy_binding":<csvserver_auditsyslogpolicy_binding
[]_value>,

"csvserver_cspolicy_binding":<csvserver_cspolicy_binding[]_value>,
```

```
"csvserver_tmtrafficpolicy_binding":<csvserver_tmtrafficpolicy_binding[]_value>

}]}
```

csvserver_botpolicy_binding

Binding object showing the botpolicy that can be bound to csvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
labelname	<String>	Read-write	Name of the label invoked.
priority	<Integer>	Read-write	Priority for the policy.
labeltype	<String>	Read-write	The invocation type. Possible values = reqvserver, resvserver, policylabel
bindpoint	<String>	Read-write	Bind point at which policy needs to be bound. Note: Content switching policies are evaluated only at request time. Possible values = REQUEST, RESPONSE, ICA_REQUEST, OTHERTCP_REQUEST,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			MQTT_JUMBO_REQ
name	<String>	Read-write	Name of the content switching virtual server to which the content switching policy applies. Minimum length = 1
policyname	<String>	Read-write	Policies bound to this vserver.
invoke	<Boolean>	Read-write	Invoke flag.
gotopriorityexpression	<String>	Read-write	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
targetlbvserver	<String>	Read-write	Name of the Load Balancing virtual server to which the content is switched, if policy rule is evaluated to be TRUE. Example: bind cs vs cs1 -policyname pol1 -priority 101 -targetLBVserver lb1 Note: Use this parameter only in case of Content Switching policy bind operations to a CS vserver. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/csvserver_botpolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"csvserver_botpolicy_binding":{

<b>"name":<String_value>,

</b>"policyname":<String_value>,

"targetlbvserver":<String_value>,

"priority":<Integer_value>,

"gotopriorityexpression":<String_value>,

"bindpoint":<String_value>,

"invoke":<Boolean_value>,

"labeltype":<String_value>,

"labelname":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver_botpolicy_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ csvserver_botpolicy_binding/ name_value<String> ? **args=policyname: <String_value> ,bindpoint: <String_value> ,priority: <Integer_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver_botpolicy_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ csvserver_botpolicy_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of csvserver_botpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/csvserver_botpolicy_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the csvserver_botpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "csvserver_botpolicy_binding": [ {

"labelname":<String_value>,

"priority":<Integer_value>,

"labeltype":<String_value>,

"bindpoint":<String_value>,

"name":<String_value>,

"policyname":<String_value>,

"invoke":<Boolean_value>,

"gotopriorityexpression":<String_value>,

"targetlbvserver":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver_botpolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/csvserver_botpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "csvserver_botpolicy_binding": [ {

"labelname":<String_value>,

"priority":<Integer_value>,

"labeltype":<String_value>,

"bindpoint":<String_value>,

"name":<String_value>,

"policyname":<String_value>,

"invoke":<Boolean_value>,

"gotopriorityexpression":<String_value>,

"targetlbvserver":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver_botpolicy_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"csvserver_botpolicy_binding": [ { "__count": "#no"} ] }
```

csvserver_cachepolicy_binding

Binding object showing the cachepolicy that can be bound to csvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
bindpoint	<String>	Read-write	The bindpoint to which the policy is bound. Possible values = REQUEST, RESPONSE, ICA_REQUEST, OTHERTCP_REQUEST, MQTT_JUMBO_REQ
labeltype	<String>	Read-write	The invocation type. Possible values = reqvserver,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			resvserver, policylabel
priority	<Integer>	Read-write	Priority for the policy.
name	<String>	Read-write	Name of the content switching virtual server to which the content switching policy applies. Minimum length = 1
labelname	<String>	Read-write	Name of the label invoked.
targetlbvserver	<String>	Read-write	Name of the Load Balancing virtual server to which the content is switched, if policy rule is evaluated to be TRUE. Example: bind cs vs cs1 -policyname pol1 -priority 101 -targetLBVserver lb1 Note: Use this parameter only in case of Content Switching policy bind operations to a CS vserver. Minimum length = 1
gotopriorityexpression	<String>	Read-write	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
invoke	<Boolean>	Read-write	Invoke flag.
policyname	<String>	Read-write	Policies bound to this vserver.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/csvserver_cachepolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"csvserver_cachepolicy_binding":{

<b>"name":<String_value>,

</b>"policyname":<String_value>,

"targetlbvserver":<String_value>,

"priority":<Integer_value>,

"gotopriorityexpression":<String_value>,

"bindpoint":<String_value>,

"invoke":<Boolean_value>,

"labeltype":<String_value>,

"labelname":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver_cachepolicy_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ csvserver_cachepolicy_binding/ name_value<String> ? **args=policyname: <String_value> ,bindpoint: <String_value> ,priority: <Integer_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver_cachepolicy_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ csvserver_cachepolicy_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of csvserver_cachepolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/csvserver_cachepolicy_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the csvserver_cachepolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "csvserver_cachepolicy_binding": [ {

"bindpoint":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"name":<String_value>,

"labelname":<String_value>,

"targetlbvserver":<String_value>,

"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>,

"policyname":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver_cachepolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ csvserver_cachepolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "csvserver_cachepolicy_binding": [ {

"bindpoint":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"name":<String_value>,

"labelname":<String_value>,

"targetlbvserver":<String_value>,

"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>,

"policyname":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver_cachepolicy_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"csvserver_cachepolicy_binding": [ { "__count": "#no"} ] }
```

csvserver_cmppolicy_binding

Binding object showing the cmppolicy that can be bound to csvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
targetlbvserver	<String>	Read-write	Name of the Load Balancing virtual server to which the content is switched, if policy rule is evaluated to be TRUE. Example: bind cs vs cs1 -policyname pol1 -priority 101

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			-targetLBVserver lb1 Note: Use this parameter only in case of Content Switching policy bind operations to a CS vserver. Minimum length = 1
policyname	<String>	Read-write	Policies bound to this vserver.
gotopriorityexpression	<String>	Read-write	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
invoke	<Boolean>	Read-write	Invoke flag.
bindpoint	<String>	Read-write	The bindpoint to which the policy is bound. Possible values = REQUEST, RESPONSE, ICA_REQUEST, OTHERTCP_REQUEST, MQTT_JUMBO_REQ
labeltype	<String>	Read-write	The invocation type. Possible values = reqvserver, resvserver, policylabel

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
priority	<Integer>	Read-write	Priority for the policy.
name	<String>	Read-write	Name of the content switching virtual server to which the content switching policy applies. Minimum length = 1
labelname	<String>	Read-write	Name of the label invoked.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/csvserver_cmppolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"csvserver_cmppolicy_binding":{

<b>"name":<String_value>,

</b>"policyname":<String_value>,

"targetlbvserver":<String_value>,

"priority":<Integer_value>,

"gotopriorityexpression":<String_value>,

"bindpoint":<String_value>,

"invoke":<Boolean_value>,

"labeltype":<String_value>,
```

```
"labelname":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver_cmppolicy_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ csvserver_cmppolicy_binding/ name_value<String> ? **args=policyname: <String_value> ,bindpoint: <String_value> ,priority: <Integer_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver_cmppolicy_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ csvserver_cmppolicy_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of csvserver_cmppolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/csvserver_cmppolicy_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the csvserver_cmppolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "csvserver_cmppolicy_binding": [ {

"targetlbvserver":<String_value>,

"policyname":<String_value>,

"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>,

"bindpoint":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"name":<String_value>,

"labelname":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver_cmppolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ csvserver_cmppolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "csvserver_cmppolicy_binding": [ {

"targetlbvserver":<String_value>,

"policyname":<String_value>,

"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>,

"bindpoint":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"name":<String_value>,

"labelname":<String_value>
```

```
}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver_cmppolicy_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"csvserver_cmppolicy_binding": [ { "__count": "#no"} ] }
```

csvserver_contentinspectionpolicy_binding

Binding object showing the contentinspectionpolicy that can be bound to csvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
bindpoint	<String>	Read-write	The bindpoint to which the policy is bound. Possible values = REQUEST, RESPONSE,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			ICA_REQUEST, OTHERTCP_REQUEST, MQTT_JUMBO_REQ
labeltype	<String>	Read-write	The invocation type. Possible values = reqvserver, resvserver, policylabel
priority	<Integer>	Read-write	Priority for the policy.
name	<String>	Read-write	Name of the content switching virtual server to which the content switching policy applies. Minimum length = 1
labelname	<String>	Read-write	Name of the label invoked.
targetlbvserver	<String>	Read-write	Name of the Load Balancing virtual server to which the content is switched, if policy rule is evaluated to be TRUE. Example: bind cs vs cs1 -policyname pol1 -priority 101 -targetLBVserver lb1 Note: Use this parameter only in case of Content Switching policy bind

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			operations to a CS vserver. Minimum length = 1
gotopriorityexpression	<String>	Read-write	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
invoke	<Boolean>	Read-write	Invoke flag.
policyname	<String>	Read-write	Policies bound to this vserver.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/csvserver_contentinspectionpolicy_binding
HTTP Method: PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"csvserver_contentinspectionpolicy_binding":{

<b>"name":<String_value>,

</b>"policyname":<String_value>,

"targetlbvserver":<String_value>,

"priority":<Integer_value>,

"gotopriorityexpression":<String_value>,
```

```
"bindpoint":<String_value>,

"invoke":<Boolean_value>,

"labeltype":<String_value>,

"labelname":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver_contentinspectionpolicy_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ csvserver_contentinspectionpolicy_binding/ name_value<String> ? **args=policyname: <String_value> ,bindpoint: <String_value> ,priority: <Integer_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver_contentinspectionpolicy_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ csvserver_contentinspectionpolicy_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of csvserver_contentinspectionpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ csvserver_contentinspectionpolicy_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the csvserver_contentinspectionpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "csvserver_contentinspectionpolicy_binding": [ {

"bindpoint":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"name":<String_value>,

"labelname":<String_value>,

"targetlbvserver":<String_value>,

"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>,

"policyname":<String_value>
```

```
}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver_contentinspectionpolicy_binding
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/csvserver_contentinspectionpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "csvserver_contentinspectionpolicy_binding": [ {

"bindpoint":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"name":<String_value>,

"labelname":<String_value>,
```

```
"targetlbvserver":<String_value>,

"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>,

"policyname":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver_contentinspectionpolicy_binding/name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"csvserver_contentinspectionpolicy_binding": [ { "__count": "#no"} ] }
```

csvserver_cspolicy_binding

Binding object showing the cspolicy that can be bound to csvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
targetlbvserver	<String>	Read-write	target vserver name.
policyname	<String>	Read-write	Policies bound to this vserver.
gotopriorityexpression	<String>	Read-write	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
invoke	<Boolean>	Read-write	Invoke flag.
name	<String>	Read-write	Name of the content switching virtual server to which the content switching policy applies. Minimum length = 1
bindpoint	<String>	Read-write	The bindpoint to which the policy is bound. Possible values = REQUEST, RESPONSE, ICA_REQUEST, OTHERTCP_REQUEST, MQTT_JUMBO_REQ
labeltype	<String>	Read-write	The invocation type. Possible values = reqvserver, resvserver, policylabel

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
priority	<Integer>	Read-write	Priority for the policy.
labelname	<String>	Read-write	Name of the label invoked.
cookieipport	<String>	Read-only	Vserver id of the lb vserver that is inserted into the set-cookie HTTP header.
hits	<Integer>	Read-only	Number of hits.
pipolicyhits	<Integer>	Read-only	Number of hits.
vserverid	<String>	Read-only	Vserver Id of vserver.
rule	<String>	Read-only	Rule.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/csvserver_cspolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"csvserver_cspolicy_binding":{

<b>"name":<String_value>,

</b>"policyname":<String_value>,

"targetlbvserver":<String_value>,

"priority":<Integer_value>,

"gotopriorityexpression":<String_value>,

"bindpoint":<String_value>,
```

```
"invoke":<Boolean_value>,

"labeltype":<String_value>,

"labelname":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver_cspolicy_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ csvserver_cspolicy_binding/ name_value<String> ? **args=policyname: <String_value> ,bindpoint: <String_value> ,priority: <Integer_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver_cspolicy_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ csvserver_cspolicy_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of csvserver_cspolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/csvserver_cspolicy_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the csvserver_cspolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "csvserver_cspolicy_binding": [ {

"targetlbvserver":<String_value>,

"policyname":<String_value>,

"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>,

"name":<String_value>,

"bindpoint":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"labelname":<String_value>,

"cookieipport":<String_value>,

"hits":<Integer_value>,
```

```
"pipolicyhits":<Integer_value>,

"vserverid":<String_value>,

"rule":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver_cspolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/csvserver_cspolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "csvserver_cspolicy_binding": [ {

"targetlbvserver":<String_value>,

"policyname":<String_value>,
```

```
"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>,

"name":<String_value>,

"bindpoint":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"labelname":<String_value>,

"cookieipport":<String_value>,

"hits":<Integer_value>,

"pipolicyhits":<Integer_value>,

"vserverid":<String_value>,

"rule":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver_cspolicy_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"csvserver_cspolicy_binding": [ { "__count": "#no"} ] }
```

csvserver_domain_binding

Binding object showing the domain that can be bound to csvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
sitedomainttl	<Integer>	Read-write	. Minimum value = 1
name	<String>	Read-write	Name of the content switching virtual server to which the content switching policy applies. Minimum length = 1
cookietimeout	<Integer>	Read-write	. Minimum value = 0 Maximum value = 1440
backupip	<String>	Read-write	. Minimum length = 1
domainname	<String>	Read-write	Domain name for which to change the time to live (TTL) and/or backup service IP address. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
cookiedomain	<String>	Read-write	. Minimum length = 1
ttl	<Integer>	Read-write	. Minimum value = 1
appflowlog	<String>	Read-only	Enable logging appflow flow information. Default value: ENABLED Possible values = ENABLED, DISABLED
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/csvserver_domain_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"csvserver_domain_binding":{

<b>"name":<String_value>,

</b>"domainname":<String_value>,

"ttl":<Integer_value>,

"backupip":<String_value>,

"cookiedomain":<String_value>,

"cookietimeout":<Integer_value>,
```

```
"sitedomainttl":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver_domain_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ csvserver_domain_binding/ name_value<String> ? **args=domainname: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver_domain_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ csvserver_domain_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of csvserver_domain_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/csvserver_domain_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the csvserver_domain_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "csvserver_domain_binding": [ {

"sitedomainttl":<Integer_value>,

"name":<String_value>,

"cookietimeout":<Integer_value>,

"backupip":<String_value>,

"domainname":<String_value>,

"cookiedomain":<String_value>,

"ttl":<Integer_value>,

"appflowlog":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver_domain_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ csvserver_domain_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "csvserver_domain_binding": [ {

"sitedomainttl":<Integer_value>,

"name":<String_value>,

"cookietimeout":<Integer_value>,

"backupip":<String_value>,

"domainname":<String_value>,

"cookiedomain":<String_value>,

"ttl":<Integer_value>,

"appflowlog":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver_domain_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"csvserver_domain_binding": [ { "__count": "#no"} ] }
```

csvserver_feopolicy_binding

Binding object showing the feopolicy that can be bound to csvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
targetlbvserver	<String>	Read-write	Name of the Load Balancing virtual server to which the content is switched, if policy rule is evaluated to be TRUE. Example: bind cs vs cs1 -policyname pol1 -priority 101

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			-targetLBVserver lb1 Note: Use this parameter only in case of Content Switching policy bind operations to a CS vserver. Minimum length = 1
policyname	<String>	Read-write	Policies bound to this vserver.
invoke	<Boolean>	Read-write	Invoke a policy label if this policy's rule evaluates to TRUE.
gotopriorityexpression	<String>	Read-write	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
priority	<Integer>	Read-write	Priority for the policy.
labeltype	<String>	Read-write	Type of label to be invoked. Possible values = reqvserver, resvserver, policylabel
bindpoint	<String>	Read-write	The bindpoint to which the policy is bound. Possible values = REQUEST, RESPONSE, ICA_REQUEST,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			OTHERTCP_REQUEST, MQTT_JUMBO_REQ
name	<String>	Read-write	Name of the content switching virtual server to which the content switching policy applies. Minimum length = 1
labelname	<String>	Read-write	Name of the label to be invoked.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/csvserver_feopolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"csvserver_feopolicy_binding":{

<b>"name":<String_value>,

</b>"policyname":<String_value>,

"targetlbvserver":<String_value>,

"priority":<Integer_value>,

"gotopriorityexpression":<String_value>,
```

```
"bindpoint":<String_value>,

"invoke":<Boolean_value>,

"labeltype":<String_value>,

"labelname":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver_feopolicy_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ csvserver_feopolicy_binding/ name_value<String> ? **args=policyname: <String_value> ,bindpoint: <String_value> ,priority: <Integer_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver_feopolicy_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ csvserver_feopolicy_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of csvserver_feopolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/csvserver_feopolicy_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the csvserver_feopolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "csvserver_feopolicy_binding": [ {

"targetlbvserver":<String_value>,

"policyname":<String_value>,

"invoke":<Boolean_value>,

"gotopriorityexpression":<String_value>,

"priority":<Integer_value>,

"labeltype":<String_value>,

"bindpoint":<String_value>,

"name":<String_value>,

"labelname":<String_value>
```

```
}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver_feopolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/csvserver_feopolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "csvserver_feopolicy_binding": [ {

"targetlbvserver":<String_value>,

"policyname":<String_value>,

"invoke":<Boolean_value>,

"gotopriorityexpression":<String_value>,

"priority":<Integer_value>,
```

```
"labeltype":<String_value>,

"bindpoint":<String_value>,

"name":<String_value>,

"labelname":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver_feopolicy_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"csvserver_feopolicy_binding": [ { "__count": "#no"} ] }
```

csvserver_gslbvserver_binding

Binding object showing the gslbvserver that can be bound to csvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the content switching virtual server to which the content switching policy applies. Minimum length = 1
vserver	<String>	Read-write	Name of the default gslb or vpn vserver bound to CS vserver of type GSLB/VPN. For Example: bind cs vserver cs1 -vserver gslb1 or bind cs vserver cs1 -vserver vpn1. Minimum length = 1
hits	<Integer>	Read-only	Number of hits.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/csvserver_gslbvserver_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"csvserver_gslbvserver_binding":{

<b>"name":<String_value>,

</b>"vserver":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver_gslbvserver_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ csvserver_gslbvserver_binding/ name_value<String> ? **args=vserver: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver_gslbvserver_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ csvserver_gslbvserver_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of csvserver_gslbvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/csvserver_gslbvserver_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the csvserver_gslbvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "csvserver_gslbvserver_binding": [ {

"name":<String_value>,

"vserver":<String_value>,

"hits":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver_gslbvserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/csvserver_gslbvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "csvserver_gslbvserver_binding": [ {

"name":<String_value>,

"vserver":<String_value>,

"hits":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver_gslbvserver_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"csvserver_gslbvserver_binding": [ { "__count": "#no"} ] }
```

csvserver_lbvserver_binding

Binding object showing the lbvserver that can be bound to csvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
targetvserver	<String>	Read-write	The virtual server name (created with the add lb vserver command) to which content will be switched. Minimum length = 1
lbvserver	<String>	Read-write	Name of the default lb vserver bound. Use this param for Default binding only. For Example: bind cs vserver cs1 -lbvserver lb1. Minimum length = 1
name	<String>	Read-write	Name of the content switching virtual server to which the content switching policy applies. Minimum length = 1
cookieipport	<String>	Read-only	Vserver id of the lb vserver that is inserted into the set-cookie HTTP header.
vserverid	<String>	Read-only	Vserver Id of vserver.
hits	<Integer>	Read-only	Number of hits.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/csvserver_lbvserver_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"csvserver_lbvserver_binding":{

<b>"name":<String_value>,

</b>"lbvserver":<String_value>,

"targetvserver":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver_lbvserver_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ csvserver_lbvserver_binding/ name_value<String> ? **args=lbvserver: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver_lbvserver_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/

csvserver_lbvserver_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of csvserver_lbvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/csvserver_lbvserver_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the csvserver_lbvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "csvserver_lbvserver_binding": [ {

"targetvserver":<String_value>,

"lbvserver":<String_value>,

"name":<String_value>,

"cookieipport":<String_value>,

"vserverid":<String_value>,

"hits":<Integer_value>
```

```
}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver_lbvserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/csvserver_lbvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "csvserver_lbvserver_binding": [ {

"targetvserver":<String_value>,

"lbvserver":<String_value>,

"name":<String_value>,

"cookieipport":<String_value>,

"vserverid":<String_value>,
```

```
"hits":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver_lbvserver_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"csvserver_lbvserver_binding": [ { "__count": "#no"} ] }
```

csvserver_responderpolicy_binding

Binding object showing the responderpolicy that can be bound to csvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the content switching virtual server to which the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			content switching policy applies. Minimum length = 1
labeltype	<String>	Read-write	The invocation type. Possible values = reqvserver, resvserver, policylabel
priority	<Integer>	Read-write	Priority for the policy.
bindpoint	<String>	Read-write	The bindpoint to which the policy is bound. Possible values = REQUEST, RESPONSE, ICA_REQUEST, OTHERTCP_REQUEST, MQTT_JUMBO_REQ
labelname	<String>	Read-write	Name of the label invoked.
targetlbvserver	<String>	Read-write	Name of the Load Balancing virtual server to which the content is switched, if policy rule is evaluated to be TRUE. Example: bind cs vs cs1 -policyname pol1 -priority 101 -targetLBVserver lb1 Note: Use this parameter only in

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			case of Content Switching policy bind operations to a CS vserver. Minimum length = 1
policyname	<String>	Read-write	Policies bound to this vserver.
gotopriorityexpression	<String>	Read-write	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
invoke	<Boolean>	Read-write	Invoke flag.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/csvserver_responderpolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"csvserver_responderpolicy_binding":{

<b>"name":<String_value>,

</b>"policyname":<String_value>,

"targetlbvserver":<String_value>,

"priority":<Integer_value>,
```

```
"gotopriorityexpression":<String_value>,

"bindpoint":<String_value>,

"invoke":<Boolean_value>,

"labeltype":<String_value>,

"labelname":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver_responderpolicy_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ csvserver_responderpolicy_binding/ name_value<String> ? **args=policyname: <String_value> ,bindpoint: <String_value> ,priority: <Integer_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver_responderpolicy_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ csvserver_responderpolicy_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of csvserver_responderpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/csvserver_responderpolicy_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the csvserver_responderpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "csvserver_responderpolicy_binding": [ {

"name":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"bindpoint":<String_value>,

"labelname":<String_value>,

"targetlbvserver":<String_value>,

"policyname":<String_value>,

"gotopriorityexpression":<String_value>,
```

```
"invoke":<Boolean_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver_responderpolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/csvserver_responderpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "csvserver_responderpolicy_binding": [ {

"name":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"bindpoint":<String_value>,
```

```
"labelname":<String_value>,

"targetlbvserver":<String_value>,

"policyname":<String_value>,

"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver_responderpolicy_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"csvserver_responderpolicy_binding": [ { "__count": "#no"} ] }
```

csvserver_rewritepolicy_binding

Binding object showing the rewritepolicy that can be bound to csvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
labelname	<String>	Read-write	Name of the label invoked.
bindpoint	<String>	Read-write	The bindpoint to which the policy is bound. Possible values = REQUEST, RESPONSE, ICA_REQUEST, OTHERTCP_REQUEST, MQTT_JUMBO_REQ
labeltype	<String>	Read-write	The invocation type. Possible values = reqvserver, resvserver, policylabel
priority	<Integer>	Read-write	Priority for the policy.
name	<String>	Read-write	Name of the content switching virtual server to which the content switching policy applies. Minimum length = 1
policyname	<String>	Read-write	Policies bound to this vserver.
gotopriorityexpression	<String>	Read-write	Expression specifying the priority of the next policy

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			which will get evaluated if the current policy rule evaluates to TRUE.
invoke	<Boolean>	Read-write	Invoke flag.
targetlbvserver	<String>	Read-write	Name of the Load Balancing virtual server to which the content is switched, if policy rule is evaluated to be TRUE. Example: bind cs vs cs1 -policyname pol1 -priority 101 -targetLBVserver lb1 Note: Use this parameter only in case of Content Switching policy bind operations to a CS vserver. Minimum length = 1
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/csvserver_rewritepolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"csvserver_rewritepolicy_binding":{

<b>"name":<String_value>,
```

```
</b>"policyname":<String_value>,

"targetlbvserver":<String_value>,

"priority":<Integer_value>,

"gotopriorityexpression":<String_value>,

"bindpoint":<String_value>,

"invoke":<Boolean_value>,

"labeltype":<String_value>,

"labelname":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver_rewritepolicy_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ csvserver_rewritepolicy_binding/ name_value<String> ? **args=policyname: <String_value> ,bindpoint: <String_value> ,priority: <Integer_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver_rewritepolicy_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ csvserver_rewritepolicy_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of csvserver_rewritepolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/csvserver_rewritepolicy_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the csvserver_rewritepolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "csvserver_rewritepolicy_binding": [ {

"labelname":<String_value>,

"bindpoint":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"name":<String_value>,
```

```
"policyname":<String_value>,

"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>,

"targetlbvserver":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver_rewritepolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/csvserver_rewritepolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "csvserver_rewritepolicy_binding": [ {

"labelname":<String_value>,
```

```
"bindpoint":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"name":<String_value>,

"policyname":<String_value>,

"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>,

"targetlbvserver":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver_rewritepolicy_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"csvserver_rewritepolicy_binding": [ { "__count": "#no"} ] }
```

csvserver_spilloverpolicy_binding

Binding object showing the spilloverpolicy that can be bound to csvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
policyname	<String>	Read-write	Policies bound to this vserver.
invoke	<Boolean>	Read-write	Invoke a policy label if this policy's rule evaluates to TRUE.
gotopriorityexpression	<String>	Read-write	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
targetlbvserver	<String>	Read-write	Name of the Load Balancing virtual server to which the content is switched, if policy rule is evaluated to be TRUE. Example: bind cs vs cs1 -policyname pol1 -priority 101 -targetLBVserver lb1 Note: Use this parameter only in case of Content Switching policy bind operations to a CS vserver. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
labelname	<String>	Read-write	Name of the label to be invoked.
name	<String>	Read-write	Name of the content switching virtual server to which the content switching policy applies. Minimum length = 1
bindpoint	<String>	Read-write	The bindpoint to which the policy is bound. Possible values = REQUEST, RESPONSE, ICA_REQUEST, OTHERTCP_REQUEST, MQTT_JUMBO_REQ
priority	<Integer>	Read-write	Priority for the policy.
labeltype	<String>	Read-write	Type of label to be invoked. Possible values = reqvserver, resvserver, policylabel
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/csvserver_spilloverpolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"csvserver_spilloverpolicy_binding":{

<b>"name":<String_value>,

</b>"policyname":<String_value>,

"targetlbvserver":<String_value>,

"priority":<Integer_value>,

"gotopriorityexpression":<String_value>,

"bindpoint":<String_value>,

"invoke":<Boolean_value>,

"labeltype":<String_value>,

"labelname":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver_spilloverpolicy_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ csvserver_spilloverpolicy_binding/ name_value<String> ? **args=policyname: <String_value> ,bindpoint: <String_value> ,priority: <Integer_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver_spilloverpolicy_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ csvserver_spilloverpolicy_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of csvserver_spilloverpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/csvserver_spilloverpolicy_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the csvserver_spilloverpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "csvserver_spilloverpolicy_binding": [ {

"policyname":<String_value>,

"invoke":<Boolean_value>,

"gotopriorityexpression":<String_value>,
```

```
"targetlbvserver":<String_value>,

"labelname":<String_value>,

"name":<String_value>,

"bindpoint":<String_value>,

"priority":<Integer_value>,

"labeltype":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver_spilloverpolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/csvserver_spilloverpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "csvserver_spilloverpolicy_binding": [ {

"policyname":<String_value>,

"invoke":<Boolean_value>,

"gotopriorityexpression":<String_value>,

"targetlbvserver":<String_value>,

"labelname":<String_value>,

"name":<String_value>,

"bindpoint":<String_value>,

"priority":<Integer_value>,

"labeltype":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver_spilloverpolicy_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"csvserver_spilloverpolicy_binding": [ { "__count": "#no"} ] }
```

csvserver_tmtrafficpolicy_binding

Binding object showing the tmtrafficpolicy that can be bound to csvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the content switching virtual server to which the content switching policy applies. Minimum length = 1
bindpoint	<String>	Read-write	Bind point at which policy needs to be bound. Note: Content switching policies are evaluated only at request time. Possible values = REQUEST, RESPONSE, ICA_REQUEST, OTHERTCP_REQUEST, MQTT_JUMBO_REQ
labeltype	<String>	Read-write	Type of label to be invoked. Possible values = reqvserver,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			resvserver, policylabel
priority	<Integer>	Read-write	Priority for the policy.
labelname	<String>	Read-write	Name of the label to be invoked.
targetlbvserver	<String>	Read-write	Name of the Load Balancing virtual server to which the content is switched, if policy rule is evaluated to be TRUE. Example: bind cs vs cs1 -policyname pol1 -priority 101 -targetLBVserver lb1 Note: Use this parameter only in case of Content Switching policy bind operations to a CS vserver. Minimum length = 1
gotopriorityexpression	<String>	Read-write	Expression or other value specifying the next policy to be evaluated if the current policy evaluates to TRUE. Specify one of the following values: * NEXT - Evaluate the policy with the next higher priority number. * END - End policy evaluation. * USE_INVOCATION_

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			RESULT - Applicable if this policy invokes another policy label. If the final goto in the invoked policy label has a value of END, the evaluation stops. If the final goto is anything other than END, the current policy label performs a NEXT. * An expression that evaluates to a number. If you specify an expression, the number to which it evaluates determines the next policy to evaluate, as follows: * If the expression evaluates to a higher numbered priority, the policy with that priority is evaluated next. * If the expression evaluates to the priority of the current policy, the policy with the next higher numbered priority is evaluated next. * If the expression evaluates to a priority number that is numerically higher than the highest numbered priority, policy

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			evaluation ends. An UNDEF event is triggered if: * The expression is invalid. * The expression evaluates to a priority number that is numerically lower than the current policy's priority. * The expression evaluates to a priority number that is between the current policy's priority number (say, 30) and the highest priority number (say, 100), but does not match any configured priority number (for example, the expression evaluates to the number 85). This example assumes that the priority number increments by 10 for every successive policy, and therefore a priority number of 85 does not exist in the policy label.
invoke	<Boolean>	Read-write	Invoke a policy label if this policy's rule evaluates to TRUE.
policyname	<String>	Read-write	Policies bound to this vserver.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/csvserver_tmtrafficpolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"csvserver_tmtrafficpolicy_binding":{

<b>"name":<String_value>,

</b>"policyname":<String_value>,

"targetlbvserver":<String_value>,

"priority":<Integer_value>,

"gotopriorityexpression":<String_value>,

"bindpoint":<String_value>,

"invoke":<Boolean_value>,

"labeltype":<String_value>,

"labelname":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver_tmtrafficpolicy_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ csvserver_tmtrafficpolicy_binding/ name_value<String> ? **args=policyname: <String_value> ,bindpoint: <String_value> ,priority: <Integer_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver_tmtrafficpolicy_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ csvserver_tmtrafficpolicy_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of csvserver_tmtrafficpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/csvserver_tmtrafficpolicy_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the csvserver_tmtrafficpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "csvserver_tmtrafficpolicy_binding": [ {

"name":<String_value>,

"bindpoint":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"labelname":<String_value>,

"targetlbvserver":<String_value>,

"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>,

"policyname":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver_tmtrafficpolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/csvserver_tmtrafficpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "csvserver_tmtrafficpolicy_binding": [ {

"name":<String_value>,

"bindpoint":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"labelname":<String_value>,

"targetlbvserver":<String_value>,

"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>,

"policyname":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver_tmtrafficpolicy_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"csvserver_tmtrafficpolicy_binding": [ { "__count": "#no"} ] }
```

csvserver_transformpolicy_binding

Binding object showing the transformpolicy that can be bound to csvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
labelname	<String>	Read-write	Name of the label invoked.
bindpoint	<String>	Read-write	The bindpoint to which the policy is bound. Possible values = REQUEST, RESPONSE, ICA_REQUEST, OTHERTCP_REQUEST, MQTT_JUMBO_REQ
labeltype	<String>	Read-write	The invocation type.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = reqvserver, resvserver, policylabel
priority	<Integer>	Read-write	Priority for the policy.
name	<String>	Read-write	Name of the content switching virtual server to which the content switching policy applies. Minimum length = 1
gotopriorityexpression	<String>	Read-write	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
invoke	<Boolean>	Read-write	Invoke flag.
policyname	<String>	Read-write	Policies bound to this vserver.
targetlbvserver	<String>	Read-write	Name of the Load Balancing virtual server to which the content is switched, if policy rule is evaluated to be TRUE. Example: bind cs vs cs1 -policyname pol1 -priority 101 -targetLBVserver lb1 Note: Use this parameter only in case of Content

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Switching policy bind operations to a CS vserver. Minimum length = 1
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/csvserver_transformpolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"csvserver_transformpolicy_binding":{

<b>"name":<String_value>,

</b>"policyname":<String_value>,

"targetlbvserver":<String_value>,

"priority":<Integer_value>,

"gotopriorityexpression":<String_value>,

"bindpoint":<String_value>,

"invoke":<Boolean_value>,

"labeltype":<String_value>,

"labelname":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver_transformpolicy_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ csvserver_transformpolicy_binding/ name_value<String> ? **args=policyname: <String_value> ,bindpoint: <String_value> ,priority: <Integer_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver_transformpolicy_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ csvserver_transformpolicy_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of csvserver_transformpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/csvserver_transformpolicy_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the csvserver_transformpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "csvserver_transformpolicy_binding": [ {

"labelname":<String_value>,

"bindpoint":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"name":<String_value>,

"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>,

"policyname":<String_value>,

"targetlbvserver":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver_transformpolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ csvserver_transformpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "csvserver_transformpolicy_binding": [ {

"labelname":<String_value>,

"bindpoint":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"name":<String_value>,

"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>,

"policyname":<String_value>,

"targetlbvserver":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver_transformpolicy_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"csvserver_transformpolicy_binding": [ { "__count": "#no"} ] }
```

csvserver_vpnvserver_binding

Binding object showing the vpnvserver that can be bound to csvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
vserver	<String>	Read-write	Name of the default gslb or vpn vserver bound to CS vserver of type GSLB/VPN. For Example: bind cs vserver cs1 -vserver gslb1 or bind cs vserver cs1 -vserver vpn1. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the content switching virtual server to which the content switching policy applies. Minimum length = 1
hits	<Integer>	Read-only	Number of hits.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/csvserver_vpnvserver_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"csvserver_vpnvserver_binding":{

<b>"name":<String_value>,

</b>"vserver":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver_vpnvserver_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ csvserver_vpnvserver_binding/ name_value<String> ? **args=vserver: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver_vpnvserver_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ csvserver_vpnvserver_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of csvserver_vpnvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/csvserver_vpnvserver_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the csvserver_vpnvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "csvserver_vpnvserver_binding": [ {

"vserver":<String_value>,

"name":<String_value>,

"hits":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver_vpnvserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/csvserver_vpnvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "csvserver_vpnvserver_binding": [ {

"vserver":<String_value>,
```

```
"name":<String_value>,

"hits":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver_vpnvserver_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"csvserver_vpnvserver_binding": [ { "__count": "#no"} ] }
```

db

Db

All the commands associated with database user

NAME	DESCRIPTION
dbdbprofile	Configuration for DB profile

NAME	DESCRIPTION
dbuser	Configuration for DB user

dbdbprofile

Configuration for DB profile resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the database profile. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at sign (@), equal sign (=), and hyphen (-) characters. Cannot be changed after the profile is created. CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my profile" or 'my profile'). .

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum length = 1 Maximum length = 127
interpretquery	<String>	Read-write	If ENABLED, inspect the query and update the connection information, if required. If DISABLED, forward the query to the server. Default value: YES Possible values = YES, NO
stickiness	<String>	Read-write	If the queries are related to each other, forward to the same backend server. Default value: NO Possible values = YES, NO
kcdaccount	<String>	Read-write	Name of the KCD account that is used for Windows authentication. Minimum length = 1 Maximum length = 127
conmultiplex	<String>	Read-write	Use the same server-side connection for multiple client-side

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			requests. Default is enabled. Default value: ENABLED Possible values = ENABLED, DISABLED
enablecachingconmuxoff	<String>	Read-write	Enable caching when connection multiplexing is OFF. Default value: DISABLED Possible values = ENABLED, DISABLED
refcnt	<Integer>	Read-only	Profile Reference Count.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/dbdbprofile **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"dbdbprofile":{

<b>"name":<String_value>,

</b>"interpretquery":<String_value>,

"stickiness":<String_value>,
```

```
"kcdaccount":<String_value>,

"conmultiplex":<String_value>,

"enablecachingconmuxoff":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/dbdbprofile/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/dbdbprofile **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"dbdbprofile":{

<b>"name":<String_value>,

</b>"interpretquery":<String_value>,
```

```
"stickiness":<String_value>,

"kcdaccount":<String_value>,

"conmultiplex":<String_value>,

"enablecachingconmuxoff":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/dbdbprofile? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"dbdbprofile":{

<b>"name":<String_value>,

</b>"interpretquery":true,

"stickiness":true,

"kcdaccount":true,

"conmultiplex":true,

"enablecachingconmuxoff":true
```

```
}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/dbdbprofile **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/dbdbprofile? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/dbdbprofile? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of dbdbprofile resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/dbdbprofile? **view=summary**

Use this query-parameter to get the summary output of dbdbprofile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/dbdbprofile? **pagesize=#no;pageno=#no**

Use this query-parameter to get the dbdbprofile resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "dbdbprofile": [ {

"name":<String_value>,

"interpretquery":<String_value>,

"stickiness":<String_value>,

"kcdaccount":<String_value>,

"conmultiplex":<String_value>,

"refcnt":<Integer_value>,

"enablecachingconmuxoff":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/dbdbprofile/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/dbdbprofile/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/dbdbprofile/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of dbdbprofile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "dbdbprofile": [ {

"name":<String_value>,

"interpretquery":<String_value>,

"stickiness":<String_value>,

"kcdaccount":<String_value>,

"conmultiplex":<String_value>,

"refcnt":<Integer_value>,

"enablecachingconmuxoff":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/dbdbprofile? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "dbdbprofile": [ { "__count": "#no"} ] }
```

dbuser

Configuration for DB user resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
username	<String>	Read-write	Name of the database user. Must be the same as the user name specified in the database. Minimum length = 1
password	<String>	Read-write	Password for logging on to the database. Must be the same as the password specified in the database. Minimum length = 1
loggedin	<Boolean>	Read-write	Display the names of all database users

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			currently logged on to the Citrix ADC.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/dbuser **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"dbuser":{

<b>"username":<String_value>,

</b>"password":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/dbuser/ username_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/dbuser **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"dbuser":{

<b>"username":<String_value>,

</b><b>"password":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/dbuser **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/dbuser? **args=username: <String_value> ,loggedin: <Boolean_value>**

Use this query-parameter to get dbuser resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/config/dbuser? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/dbuser? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of dbuser resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/dbuser? **view=summary**

Use this query-parameter to get the summary output of dbuser resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/dbuser? **pagesize=#no;pageno=#no**

Use this query-parameter to get the dbuser resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "dbuser": [ {

username:<String_value>,loggedin:<Boolean_value>"_nextgenapiresource":<Str
ing_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/dbuser/ username_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/dbuser/ username_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/dbuser/ username_value<String> ? **view=summary**

Use this query-parameter to get the summary output of dbuser resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "dbuser": [ {

username:<String_value>,loggedin:<Boolean_value>"_nextgenapiresource":<Str
ing_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/dbuser? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "dbuser": [ { "__count": "#no"} ] }
```

dns

Domain Name Service

Domain Name Service(DNS) configuration.

NAME	DESCRIPTION
dnsaaaarec	Configuration for IPv6 address type record
dnsaction	Configuration for DNS action
dnsaction64	Configuration for dns64 action
dnsaddrec	Configuration for address type record
dnscaarec	Configuration for CAA record
dnscnamerec	Configuration for CNAME record
dnsdsfile	Configuration for dnskey dsfile
dnsglobal_binding	Binding object showing the resources that can be bound to dnsglobal
dnsglobal_dnspolicy_binding	Binding object showing the dnspolicy that can be bound to dnsglobal
dnskey	Configuration for dns key

NAME	DESCRIPTION
dnsmxrec	Configuration for MX record
dnsnameserver	Configuration for name server
dnsnaptrrec	Configuration for NAPTR record
dnsnegativecacherecords	Configuration for Negative Cache Records
dnsnsecrec	
dnsnsrec	Configuration for name server record
dnsparameter	Configuration for DNS parameter
dnspolicy	Configuration for DNS policy
dnspolicy64	Configuration for dns64 policy
dnspolicy64_binding	Binding object showing the resources that can be bound to dnspolicy64
dnspolicy64_lbvserver_binding	Binding object showing the lbvserver that can be bound to dnspolicy64
dnspolicy_binding	Binding object showing the resources that can be bound to dnspolicy
dnspolicy_dnsglobal_binding	Binding object showing the dnsglobal that can be bound to dnspolicy
dnspolicy_dnspolicylabel_binding	Binding object showing the dnspolicylabel that can be bound to dnspolicy
dnspolicylabel	Configuration for dns policy label
dnspolicylabel_binding	Binding object showing the resources that can be bound to dnspolicylabel

NAME	DESCRIPTION
dnspolicylabel_dnspolicy_binding	Binding object showing the dnspolicy that can be bound to dnspolicylabel
dnspolicylabel_policybinding_binding	Binding object showing the policybinding that can be bound to dnspolicylabel
dnsprofile	Configuration for DNS profile
dnsproxyrecords	Configuration for proxy record
dnsptrrec	Configuration for PTR record
dnsresolverentry	Configuration for Active DNS resolution entries
dnssoarec	Configuration for SOA record
dnssrvrec	Configuration for server record
dnssubnetcache	Configuration for subnet cache
dnssuffix	Configuration for DNS suffix
dnssvcbrec	Configuration for SVCB/HTTPS service binding record
dnstxtrec	Configuration for TXT record
dnsview	Configuration for DNS view
dnsview_binding	Binding object showing the resources that can be bound to dnsview
dnsview_dnspolicy_binding	Binding object showing the dnspolicy that can be bound to dnsview
dnsview_gslbservice_binding	Binding object showing the gslbservice that can be bound to dnsview

NAME	DESCRIPTION
dnszone	Configuration for DNS zone
dnszone_binding	Binding object showing the resources that can be bound to dnszone
dnszone_dnskey_binding	Binding object showing the dnskey that can be bound to dnszone
dnszone_domain_binding	Binding object showing the domain that can be bound to dnszone

dnsaaaarec

Configuration for IPv6 address type record resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
hostname	<String>	Read-write	Domain name. Minimum length = 1
ipv6address	<String>	Read-write	One or more IPv6 addresses to assign to the domain name. Minimum length = 1
ttl	<Integer>	Read-write	Time to Live (TTL), in seconds, for the record. TTL is the time for which the record must be cached by DNS proxies. The specified TTL is applied to all the resource records that are of the same record type and

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			belong to the specified domain name. For example, if you add an address record, with a TTL of 36000, to the domain name example.com, the TTLs of all the address records of example.com are changed to 36000. If the TTL is not specified, the Citrix ADC uses either the DNS zone's minimum TTL or, if the SOA record is not available on the appliance, the default value of 3600. Default value: 3600 Minimum value = 0 Maximum value = 2147483647
ecssubnet	<String>	Read-write	Subnet for which the cached records need to be removed.
type	<String>	Read-write	Type of records to display. Available settings function as follows: * ADNS - Display all authoritative address records.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			* PROXY - Display all proxy address records. * ALL - Display all address records. Possible values = ALL, ADNS, PROXY
nodeid	<Integer>	Read-write	Unique number that identifies the cluster node. Minimum value = 0 Maximum value = 31
vservername	<String>	Read-only	Vitual server name.
authtype	<String>	Read-only	Authentication type. Possible values = ALL, ADNS, PROXY
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnsaaaarec **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"dnsaaaarec":{

<b>"hostname":<String_value>,

</b><b>"ipv6address":<String_value>,

</b>"ttl":<Integer_value>
```

```
}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnsaaaarec/ hostname_value<String> **Query-parameters: args=ecssubnet: <String_value> ,ipv6address: <String_value>**
get (all)
URL: http:// <netscaler-ip-address> /nitro/v1/config/dnsaaaarec **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/dnsaaaarec? **args=hostname: <String_value> ,ipv6address: <String_value> ,type: <String_value> ,nodeid: <Integer_value>**

Use this query-parameter to get dnsaaaarec resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/config/dnsaaaarec? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/dnsaaaarec? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of dnsaaaarec resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/dnsaaaarec? **view=summary**

Use this query-parameter to get the summary output of dnsaaaarec resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/dnsaaaarec? **pagesize=#no;pageno=#no**

Use this query-parameter to get the dnsaaaarec resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "dnsaaaarec": [ {

hostname:<String_value>,ipv6address:<String_value>,type:<String_value>,nod
eid:<Integer_value>"ecssubnet":<String_value>,

"ttl":<Integer_value>,

"vservername":<String_value>,

"authtype":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

count

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnsaaaarec? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "dnsaaaarec": [ { "__count": "#no"} ] }
```

dnsaction

Configuration for DNS action resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
actionname	<String>	Read-write	Name of the dns action.
actiontype	<String>	Read-write	The type of DNS action that is being configured. Possible values = ViewName, GslbPrefLoc, noop, Drop, Cache_Bypass, Rewrite_Response
ipaddress	<String[]>	Read-write	List of IP address to be returned in case of rewrite_response actiontype. They can be of IPV4 or IPV6 type.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			In case of set command We will remove all the IP address previously present in the action and will add new once given in set dns action command.
ttl	<Integer>	Read-write	Time to live, in seconds. Default value: 3600 Minimum value = 0 Maximum value = 2147483647
viewname	<String>	Read-write	The view name that must be used for the given action.
preferredloclist	<String[]>	Read-write	The location list in priority order used for the given action. Minimum length = 1
dnsprofilename	<String>	Read-write	Name of the DNS profile to be associated with the transaction for which the action is chosen. Minimum length = 1 Maximum length = 127
drop	<String>	Read-only	The dns packet must be dropped.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = YES, NO
cachebypass	<String>	Read-only	By pass dns cache for this. Possible values = YES, NO
builtin	<String[]>	Read-only	Flag to determine whether DNS action is default or not. Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL
feature	<String>	Read-only	The feature to be checked while applying this config.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnsaction **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"dnsaction":{

<b>"actionname":<String_value>,

</b><b>"actiontype":<String_value>,

</b>"ipaddress":<String[]_value>,
```

```
"ttl":<Integer_value>,

"viewname":<String_value>,

"preferredloclist":<String[]_value>,

"dnsprofilename":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnsaction/ actionname_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnsaction **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"dnsaction":{

<b>"actionname":<String_value>,
```

```
</b>"ipaddress":<String[]_value>,

"ttl":<Integer_value>,

"viewname":<String_value>,

"preferredloclist":<String[]_value>,

"dnsprofilename":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnsaction? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"dnsaction":{

<b>"actionname":<String_value>,

</b>"ttl":true,

"dnsprofilename":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnsaction **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/dnsaction? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/dnsaction? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of dnsaction resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/dnsaction? **view=summary**

Use this query-parameter to get the summary output of dnsaction resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/dnsaction? **pagesize=#no;pageno=#no**

Use this query-parameter to get the dnsaction resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "dnsaction": [ {

"actionname":<String_value>,

"actiontype":<String_value>,

"ttl":<Integer_value>,

"ipaddress":<String[]_value>,

"viewname":<String_value>,

"preferredloclist":<String[]_value>,

"drop":<String_value>,

"cachebypass":<String_value>,

"dnsprofilename":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnsaction/ actionname_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/dnsaction/ actionname_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/dnsaction/ actionname_value<String> ? **view=summary**

Use this query-parameter to get the summary output of dnsaction resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "dnsaction": [ {

"actionname":<String_value>,

"actiontype":<String_value>,

"ttl":<Integer_value>,

"ipaddress":<String[]_value>,

"viewname":<String_value>,

"preferredloclist":<String[]_value>,

"drop":<String_value>,

"cachebypass":<String_value>,

"dnsprofilename":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,
```

```
"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnsaction? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "dnsaction": [ { "__count": "#no"} ] }
```

dnsaction64

Configuration for dns64 action resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
actionname	<String>	Read-write	Name of the dns64 action.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
prefix	<String>	Read-write	The dns64 prefix to be used if the after evaluating the rules.
mappedrule	<String>	Read-write	The expression to select the criteria for ipv4 addresses to be used for synthesis. Only if the mappedrule is evaluated to true the corresponding ipv4 address is used for synthesis using respective prefix, otherwise the A RR is discarded.
excluderule	<String>	Read-write	The expression to select the criteria for eliminating the corresponding ipv6 addresses from the response.
builtin	<String[]>	Read-only	Flag to determine whether dna64action is default or not. Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL
feature	<String>	Read-only	The feature to be checked while applying this config.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnsaction64 **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"dnsaction64":{

<b>"actionname":<String_value>,

</b><b>"prefix":<String_value>,

</b>"mappedrule":<String_value>,

"excluderule":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnsaction64/ actionname_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnsaction64 **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"dnsaction64":{

<b>"actionname":<String_value>,

</b>"prefix":<String_value>,

"mappedrule":<String_value>,

"excluderule":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnsaction64? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"dnsaction64":{

<b>"actionname":<String_value>,

</b>"prefix":true,

"mappedrule":true,

"excluderule":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnsaction64 **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/dnsaction64? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/dnsaction64? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of dnsaction64 resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/dnsaction64? **view=summary**

Use this query-parameter to get the summary output of dnsaction64 resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/dnsaction64? **pagesize=#no;pageno=#no**

Use this query-parameter to get the dnsaction64 resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "dnsaction64": [ {

"actionname":<String_value>,

"prefix":<String_value>,

"mappedrule":<String_value>,

"excluderule":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnsaction64/ actionname_value<String>
Query-parameters: attrs http:// <netscaler-ip-address> /nitro/v1/config/dnsaction64/ actionname_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/dnsaction64/ actionname_value<String> ? **view=summary**

Use this query-parameter to get the summary output of dnsaction64 resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "dnsaction64": [ {

"actionname":<String_value>,

"prefix":<String_value>,

"mappedrule":<String_value>,

"excluderule":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

```
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnsaction64? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "dnsaction64": [ { "__count": "#no"} ] }
```

dnsaddrec

Configuration for address type record resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
hostname	<String>	Read-write	Domain name. Minimum length = 1
ipaddress	<String>	Read-write	One or more IPv4 addresses to assign to the domain name. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ttl	<Integer>	Read-write	Time to Live (TTL), in seconds, for the record. TTL is the time for which the record must be cached by DNS proxies. The specified TTL is applied to all the resource records that are of the same record type and belong to the specified domain name. For example, if you add an address record, with a TTL of 36000, to the domain name example.com, the TTLs of all the address records of example.com are changed to 36000. If the TTL is not specified, the Citrix ADC uses either the DNS zone's minimum TTL or, if the SOA record is not available on the appliance, the default value of 3600. Default value: 3600 Minimum value = 0 Maximum value = 2147483647

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ecssubnet	<String>	Read-write	Subnet for which the cached address records need to be removed.
type	<String>	Read-write	The address record type. The type can take 3 values: ADNS - If this is specified, all of the authoritative address records will be displayed. PROXY - If this is specified, all of the proxy address records will be displayed. ALL - If this is specified, all of the address records will be displayed. Possible values = ALL, ADNS, PROXY
nodeid	<Integer>	Read-write	Unique number that identifies the cluster node. Minimum value = 0 Maximum value = 31
vservername	<String>	Read-only	Vitual server name.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
authtype	<String>	Read-only	Authentication type. Possible values = ALL, ADNS, PROXY
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnsaddrec **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"dnsaddrec":{

<b>"hostname":<String_value>,

</b><b>"ipaddress":<String_value>,

</b>"ttl":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnsaddrec/ hostname_value<String> **Query-parameters: args=ecssubnet: <String_value> ,ipaddress: <String_value>**
get (all)
URL: http:// <netscaler-ip-address> /nitro/v1/config/dnsaddrec **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/dnsaddrec? **args=hostname: <String_value> ,type: <String_value> ,nodeid: <Integer_value>**

Use this query-parameter to get dnsaddrec resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/config/dnsaddrec? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/dnsaddrec? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of dnsaddrec resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/dnsaddrec? **view=summary**

Use this query-parameter to get the summary output of dnsaddrec resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/dnsaddrec? **pagesize=#no;pageno=#no**

Use this query-parameter to get the dnsaddrec resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "dnsaddrec": [ {

hostname:<String_value>,type:<String_value>,nodeid:<Integer_value>"ipaddre
ss":<String_value>,

"ecssubnet":<String_value>,

"ttl":<Integer_value>,

"vservername":<String_value>,

"authtype":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

get
URL: http:// <netscaler-ip-address> /nitro/v1/config/dnsaddrec/ hostname_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/dnsaddrec/ hostname_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/dnsaddrec/ hostname_value<String> ? **view=summary**

Use this query-parameter to get the summary output of dnsaddrec resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "dnsaddrec": [ {

hostname:<String_value>,type:<String_value>,nodeid:<Integer_value>"ipaddre
ss":<String_value>,

"ecssubnet":<String_value>,

"ttl":<Integer_value>,

"vservername":<String_value>,

"authtype":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

count
URL: http:// <netscaler-ip-address> /nitro/v1/config/dnsaddrec? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "dnsaddrec": [ { "__count": "#no"} ] }
```

dnscaarec

Configuration for CAA record resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
domain	<String>	Read-write	Domain name of the CAA record. Minimum length = 1
valuestring	<String>	Read-write	Value associated with the chosen property tag in the CAA resource record. Enclose the string in single or double quotation marks. Minimum length = 1
tag	<String>	Read-write	String that represents the identifier of the property represented by the CAA record. The RFC currently defines three available tags - issue, issuwild and iodef. Default value: "issue"

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum length = 1 Maximum length = 255
flag	<String>	Read-write	Flag associated with the CAA record. Default value: 5 Possible values = NONE, CRITICAL
ttl	<Integer>	Read-write	Time to Live (TTL), in seconds, for the record. TTL is the time for which the record must be cached by DNS proxies. The specified TTL is applied to all the resource records that are of the same record type and belong to the specified domain name. For example, if you add an address record, with a TTL of 36000, to the domain name example.com, the TTLs of all the address records of example.com are changed to 36000. If the TTL is not specified, the Citrix ADC uses either the DNS zone's minimum TTL or, if

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			the SOA record is not available on the appliance, the default value of 3600. Default value: 3600 Minimum value = 0 Maximum value = 2147483647
recordid	<Integer>	Read-write	Unique, internally generated record ID. View the details of the CAA record to obtain its record ID. Records can be removedby either specifying the domain name and record id OR by specifying domain name and all other CAA record attributes as was supplied during the add command. Minimum value = 1 Maximum value = 65535
ecssubnet	<String>	Read-write	Subnet for which the cached CAA record need to be removed.
type	<String>	Read-write	Type of records to display. Available settings function as follows:

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			* ADNS - Display all authoritative address records. * PROXY - Display all proxy address records. * ALL - Display all address records. Default value: ADNS Possible values = ALL, ADNS, PROXY
nodeid	<Integer>	Read-write	Unique number that identifies the cluster node. Minimum value = 0 Maximum value = 31
authtype	<String>	Read-only	Authentication type. Possible values = ALL, ADNS, PROXY
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD

- DELETE
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnscaarec **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"dnscaarec":{

<b>"domain":<String_value>,

</b><b>"valuestring":<String_value>,

</b>"tag":<String_value>,

"flag":<String_value>,

"ttl":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnscaarec/ domain_value<String> **Query-parameters: args=valuestring: <String_value> ,recordid: <Integer_value> ,tag: <String_value> ,flag: <String_value> ,ecssubnet: <String_value>**
get (all)
URL: http:// <netscaler-ip-address> /nitro/v1/config/dnscaarec **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/dnscaarec? **args=domain: <String_value> ,type: <String_value> ,nodeid: <Integer_value>**

Use this query-parameter to get dnscaarec resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/config/dnscaarec? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/dnscaarec? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of dnscaarec resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/dnscaarec? **view=summary**

Use this query-parameter to get the summary output of dnscaarec resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/dnscaarec? **pagesize=#no;pageno=#no**

Use this query-parameter to get the dnscaarec resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "dnscaarec": [ {

domain:<String_value>,type:<String_value>,nodeid:<Integer_value>"valuestri
ng":<String_value>,

"tag":<String_value>,

"flag":<String_value>,

"ecssubnet":<String_value>,

"ttl":<Integer_value>,

"recordid":<Integer_value>,
```

```
"authtype":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

get
URL: http:// <netscaler-ip-address> /nitro/v1/config/dnscaarec/ domain_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/dnscaarec/ domain_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/dnscaarec/ domain_value<String> ? **view=summary**

Use this query-parameter to get the summary output of dnscaarec resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "dnscaarec": [ {

domain:<String_value>,type:<String_value>,nodeid:<Integer_value>"valuestri
ng":<String_value>,

"tag":<String_value>,

"flag":<String_value>,

"ecssubnet":<String_value>,

"ttl":<Integer_value>,

"recordid":<Integer_value>,

"authtype":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

count

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnscaarec? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "dnscaarec": [ { "__count": "#no"} ] }
```

dnscnamerec

Configuration for CNAME record resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
aliasname	<String>	Read-write	Alias for the canonical domain name. Minimum length = 1
canonicalname	<String>	Read-write	Canonical domain name. Minimum length = 1
ttl	<Integer>	Read-write	Time to Live (TTL), in seconds, for the record. TTL is the time for which the record must be cached by DNS proxies. The specified TTL is applied to all the resource records that are of the same record type and belong to the specified domain name. For example, if you add an address record, with a TTL of 36000, to the domain name example.com, the TTLs of all the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			address records of example.com are changed to 36000. If the TTL is not specified, the Citrix ADC uses either the DNS zone's minimum TTL or, if the SOA record is not available on the appliance, the default value of 3600. Default value: 3600 Minimum value = 0 Maximum value = 2147483647
ecssubnet	<String>	Read-write	Subnet for which the cached CNAME record need to be removed.
type	<String>	Read-write	Type of records to display. Available settings function as follows: * ADNS - Display all authoritative address records. * PROXY - Display all proxy address records. * ALL - Display all address records.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: ADNS Possible values = ALL, ADNS, PROXY
nodeid	<Integer>	Read-write	Unique number that identifies the cluster node. Minimum value = 0 Maximum value = 31
vservername	<String>	Read-only	GSLB Vitual server name to which this domain is bound.
authtype	<String>	Read-only	Record type. Possible values = ALL, ADNS, PROXY
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnscnamerec **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"dnscnamerec":{

<b>"aliasname":<String_value>,

</b><b>"canonicalname":<String_value>,

</b>"ttl":<Integer_value>
```

```
}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnscnamerec/ aliasname_value<String>
Query-parameters: args=ecssubnet: <String_value>
get (all)
URL: http:// <netscaler-ip-address> /nitro/v1/config/dnscnamerec **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/dnscnamerec? **args=aliasname: <String_value> ,type: <String_value> ,nodeid: <Integer_value>**

Use this query-parameter to get dnscnamerec resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/config/dnscnamerec? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/dnscnamerec? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of dnscnamerec resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/dnscnamerec? **view=summary**

Use this query-parameter to get the summary output of dnscnamerec resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/dnscnamerec? **pagesize=#no;pageno=#no**

Use this query-parameter to get the dnscnamerec resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "dnscnamerec": [ {

aliasname:<String_value>,type:<String_value>,nodeid:<Integer_value>"canoni
calname":<String_value>,

"ttl":<Integer_value>,

"vservername":<String_value>,

"authtype":<String_value>,

"ecssubnet":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

get
URL: http:// <netscaler-ip-address> /nitro/v1/config/dnscnamerec/ aliasname_value<String>
Query-parameters: attrs http:// <netscaler-ip-address> /nitro/v1/config/dnscnamerec/ aliasname_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/dnscnamerec/ aliasname_value<String> ? **view=summary**

Use this query-parameter to get the summary output of dnscnamerec resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "dnscnamerec": [ {

aliasname:<String_value>,type:<String_value>,nodeid:<Integer_value>"canoni
calname":<String_value>,

"ttl":<Integer_value>,

"vservername":<String_value>,

"authtype":<String_value>,

"ecssubnet":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

count

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnscnamerec? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "dnscnamerec": [ { "__count": "#no"} ] }
```

dnsdsfile

Configuration for dnskey dsfile resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
keyname	<String>	Read-write	Name of the DNS key. Minimum length = 1
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnsdsfile **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/dnsdsfile? **args=keyname: <String_value>**

Use this query-parameter to get dnsdsfile resources based on additional properties.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "dnsdsfile": [ {

keyname:<String_value>"_nextgenapiresource":<String_value>

}]}
```

dnsglobal_binding

Binding object which returns the resources bound to dnsglobal.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
dnsglobal_dnspolicy_binding	<dnsglobal_dnspolicy_binding[]>	Read-write	dnspolicy that can be bound to dnsglobal.

Operations

(click to see Properties)

- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnsglobal_binding

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "dnsglobal_binding": [ {

"dnsglobal_dnspolicy_binding":<dnsglobal_dnspolicy_binding[]_value>

}]}
```

dnsglobal_dnspolicy_binding

Binding object showing the dnspolicy that can be bound to dnsglobal.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
type	<String>	Read-write	Type of global bind point for which to show bound policies. Possible values = REQ_OVERRIDE, REQ_DEFAULT, RES_OVERRIDE, RES_DEFAULT
gotopriorityexpression	<String>	Read-write	Expression or other value specifying the next policy to be evaluated if the current policy evaluates to TRUE. Specify one of the following values: * NEXT - Evaluate the policy with the next higher priority number. * END - End policy evaluation. * USE_INVOCATION_

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			RESULT - Applicable if this policy invokes another policy label. If the final goto in the invoked policy label has a value of END, the evaluation stops. If the final goto is anything other than END, the current policy label performs a NEXT. * An expression that evaluates to a number. If you specify an expression, the number to which it evaluates determines the next policy to evaluate, as follows: * If the expression evaluates to a higher numbered priority, the policy with that priority is evaluated next. * If the expression evaluates to the priority of the current policy, the policy with the next higher numbered priority is evaluated next. * If the expression evaluates to a priority number that is numerically higher than the highest numbered priority, policy

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			evaluation ends. An UNDEF event is triggered if: * The expression is invalid. * The expression evaluates to a priority number that is numerically lower than the current policy's priority. * The expression evaluates to a priority number that is between the current policy's priority number (say, 30) and the highest priority number (say, 100), but does not match any configured priority number (for example, the expression evaluates to the number 85). This example assumes that the priority number increments by 10 for every successive policy, and therefore a priority number of 85 does not exist in the policy label. Minimum length = 1
invoke	<Boolean>	Read-write	Invoke flag.
policyname	<String>	Read-write	Name of the dns policy.
globalbindtype	<String>	Read-write	.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: SYSTEM_GLOBAL Possible values = SYSTEM_GLOBAL, VPN_GLOBAL, RNAT_GLOBAL, APPFW_GLOBAL, TM_GLOBAL
labeltype	<String>	Read-write	Type of policy label invocation. Possible values = policylabel
priority	<Integer>	Read-write	Specifies the priority of the policy with which it is bound. Maximum allowed priority should be less than 65535.
labelname	<String>	Read-write	Name of the label to invoke if the current policy rule evaluates to TRUE.
flowtype	<Integer>	Read-only	flowtype of the bound rewrite policy.
numpol	<Integer>	Read-only	The number of policies bound to the bindpoint.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD

- DELETE
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/dnsglobal_dnspolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"dnsglobal_dnspolicy_binding":{

<b>"policyname":<String_value>,

</b><b>"priority":<Integer_value>,

</b>"gotopriorityexpression":<String_value>,

"type":<String_value>,

"invoke":<Boolean_value>,

"labeltype":<String_value>,

"labelname":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnsglobal_dnspolicy_binding **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/dnsglobal_dnspolicy_binding? **args= policyname:<String_value>, type: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnsglobal_dnspolicy_binding **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/dnsglobal_dnspolicy_binding? **args=type: <String_value>**

Use this query-parameter to get dnsglobal_dnspolicy_binding resources based on additional properties.

filter http:// <netscaler-ip-address> /nitro/v1/config/dnsglobal_dnspolicy_binding? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of dnsglobal_dnspolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/dnsglobal_dnspolicy_binding? **pagesize=#no;pageno=#no**

Use this query-parameter to get the dnsglobal_dnspolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "dnsglobal_dnspolicy_binding": [ {

"type":<String_value>,

"gotopriorityexpression":<String_value>,
```

```
"invoke":<Boolean_value>,

"policyname":<String_value>,

"globalbindtype":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"labelname":<String_value>,

"flowtype":<Integer_value>,

"numpol":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnsglobal_dnspolicy_binding? **count=yes**
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "dnsglobal_dnspolicy_binding": [ { "__count": "#no"} ] }
```

dnskey

Configuration for dns key resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
keyname	<String>	Read-write	Name of the public-private key pair to publish in the zone. Minimum length = 1
publickey	<String>	Read-write	File name of the public key.
privatekey	<String>	Read-write	File name of the private key.
expires	<Integer>	Read-write	Time period for which to consider the key valid, after the key is used to sign a zone. Default value: 120 Minimum value = 1 Maximum value = 32767
units1	<String>	Read-write	Units for the expiry period. Default value: DAYS Possible values = MINUTES, HOURS, DAYS
notificationperiod	<Integer>	Read-write	Time at which to generate notification

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			of key expiration, specified as number of days, hours, or minutes before expiry. Must be less than the expiry period. The notification is an SNMP trap sent to an SNMP manager. To enable the appliance to send the trap, enable the DNSKEY-EXPIRY SNMP alarm. In case autorollover option is enabled, rollover for successor key will be intiated at this time. No notification trap will be sent. Default value: 7 Minimum value = 1 Maximum value = 32767
units2	<String>	Read-write	Units for the notification period. Default value: DAYS Possible values = MINUTES, HOURS, DAYS

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ttl	<Integer>	Read-write	Time to Live (TTL), in seconds, for the DNSKEY resource record created in the zone. TTL is the time for which the record must be cached by the DNS proxies. If the TTL is not specified, either the DNS zone's minimum TTL or the default value of 3600 is used. Default value: 3600 Minimum value = 0 Maximum value = 2147483647
password	<String>	Read-write	Passphrase for reading the encrypted public/ private DNS keys. Minimum length = 1
autorollover	<String>	Read-write	Flag to enable/ disable key rollover automatically. Note: * Key name will be appended with _AR1 for successor key. For e.g. current key=k1, successor key=k1_AR1.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			* Key name can be truncated if current name length is more than 58 bytes to accomodate the suffix. Default value: DISABLED Possible values = ENABLED, DISABLED
rollovermethod	<String>	Read-write	Method used for automatic rollover. * Key type: ZSK, Method: PrePublication or DoubleSignature. * Key type: KSK, Method: DoubleRRSet. Possible values = PrePublication, DoubleSignature, DoubleRRSet
revoke	<Boolean>	Read-write	Revoke the key. Note: This operation is non-reversible.
zonename	<String>	Read-write	Name of the zone for which to create a key. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
keytype	<String>	Read-write	Type of key to create. Default value: ZSK Possible values = KSK, KeySigningKey, ZSK, ZoneSigningKey
algorithm	<String>	Read-write	Algorithm to generate the key. Default value: NS_DNSKEYALGO_RSASHA1 Possible values = RSASHA1, RSASHA256, RSASHA512
keysize	<Integer>	Read-write	Size of the key, in bits. Default value: 512 Minimum value = 1 Maximum value = 4096
filenameprefix	<String>	Read-write	Common prefix for the names of the generated public and private key files and the Delegation Signer (DS) resource record. During key generation, the .key, .private, and .ds suffixes are

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			appended automatically to the file name prefix to produce the names of the public key, the private key, and the DS record, respectively. Minimum length = 1 Maximum length = 55
src	<String>	Read-write	URL (protocol, host, path, and file name) from where the DNS key file will be imported. NOTE: The import fails if the object to be imported is on an HTTPS server that requires client certificate authentication for access. This is a mandatory argument. Minimum length = 1 Maximum length = 2047
state	<String>	Read-only	Current key state. Default value: Created Possible values = Created, Activated, Deactivated, Revoked

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
type	<String>	Read-only	Key type. Default value: ZSK Possible values = KSK, KeySigningKey, ZSK, ZoneSigningKey
tag	<Integer>	Read-only	Key tag/ID. Default value: 0
createtimestr	<String>	Read-only	Key creation time. Default value: 0
activationtimestr	<String>	Read-only	Key activation time. Default value: 0
expirytimestr	<String>	Read-only	Key expiry time. Default value: 0
deletiontimestr	<String>	Read-only	Key deletion time if autorollover option is enabled. Default value: 0
rolloverfailrc	<Integer>	Read-only	Reason code in case rollover event failed. Default value: 0
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- CREATE

- UPDATE
- UNSET
- DELETE
- GET (ALL)
- GET
- COUNT
- IMPORT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnskey **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"dnskey":{

<b>"keyname":<String_value>,

</b><b>"publickey":<String_value>,

</b><b>"privatekey":<String_value>,

</b>"expires":<Integer_value>,

"units1":<String_value>,

"notificationperiod":<Integer_value>,

"units2":<String_value>,

"ttl":<Integer_value>,

"password":<String_value>,

"autorollover":<String_value>,

"rollovermethod":<String_value>,

"revoke":<Boolean_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

CREATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnskey? **action=create HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"dnskey":{

<b>"zonename":<String_value>,

</b><b>"keytype":<String_value>,

</b><b>"algorithm":<String_value>,

</b><b>"keysize":<Integer_value>,

</b><b>"filenameprefix":<String_value>,

</b>"password":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnskey **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"dnskey":{

<b>"keyname":<String_value>,

</b>"expires":<Integer_value>,

"units1":<String_value>,

"notificationperiod":<Integer_value>,

"units2":<String_value>,

"ttl":<Integer_value>,

"autorollover":<String_value>,

"rollovermethod":<String_value>,

"revoke":<Boolean_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnskey? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"dnskey":{

<b>"keyname":<String_value>,
```

```
</b>"expires":true,

"units1":true,

"notificationperiod":true,

"units2":true,

"ttl":true,

"autorollover":true,

"rollovermethod":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnskey/ keyname_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

IMPORT

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnskey? **action=Import HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"dnskey":{

<b>"keyname":<String_value>,

</b><b>"src":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnskey **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/dnskey? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/dnskey? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of dnskey resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/dnskey? **view=summary**

Use this query-parameter to get the summary output of dnskey resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/dnskey? **pagesize=#no;pageno=#no**

Use this query-parameter to get the dnskey resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "dnskey": [ {

"keyname":<String_value>,

"publickey":<String_value>,

"privatekey":<String_value>,

"expires":<Integer_value>,

"units1":<String_value>,

"notificationperiod":<Integer_value>,

"units2":<String_value>,

"ttl":<Integer_value>,

"zonename":<String_value>,

"password":<String_value>,

"autorollover":<String_value>,

"rollovermethod":<String_value>,

"state":<String_value>,

"type":<String_value>,

"tag":<Integer_value>,
```

```
"createtimestr":<String_value>,

"activationtimestr":<String_value>,

"expirytimestr":<String_value>,

"deletiontimestr":<String_value>,

"rolloverfailrc":<Integer_value>,

"revoke":<Boolean_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnskey/ keyname_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/dnskey/ keyname_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/dnskey/ keyname_value<String> ? **view=summary**

Use this query-parameter to get the summary output of dnskey resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "dnskey": [ {

"keyname":<String_value>,

"publickey":<String_value>,

"privatekey":<String_value>,

"expires":<Integer_value>,

"units1":<String_value>,

"notificationperiod":<Integer_value>,

"units2":<String_value>,

"ttl":<Integer_value>,

"zonename":<String_value>,

"password":<String_value>,

"autorollover":<String_value>,

"rollovermethod":<String_value>,

"state":<String_value>,

"type":<String_value>,

"tag":<Integer_value>,

"createtimestr":<String_value>,

"activationtimestr":<String_value>,

"expirytimestr":<String_value>,
```

```
"deletiontimestr":<String_value>,

"rolloverfailrc":<Integer_value>,

"revoke":<Boolean_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnskey? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "dnskey": [ { "__count": "#no"} ] }
```

dnsmxrec

Configuration for MX record resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
domain	<String>	Read-write	Domain name for which to add the MX record. Minimum length = 1
mx	<String>	Read-write	Host name of the mail exchange server. Minimum length = 1
pref	<Integer>	Read-write	Priority number to assign to the mail exchange server. A domain name can have multiple mail servers, with a priority number assigned to each server. The lower the priority number, the higher the mail server's priority. When other mail servers have to deliver mail to the specified domain, they begin with the mail server with the lowest priority number, and use other configured mail servers, in priority order, as backups. Minimum value = 0 Maximum value = 65535
ttl	<Integer>	Read-write	Time to Live (TTL), in seconds, for the record. TTL is the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			time for which the record must be cached by DNS proxies. The specified TTL is applied to all the resource records that are of the same record type and belong to the specified domain name. For example, if you add an address record, with a TTL of 36000, to the domain name example.com, the TTLs of all the address records of example.com are changed to 36000. If the TTL is not specified, the Citrix ADC uses either the DNS zone's minimum TTL or, if the SOA record is not available on the appliance, the default value of 3600. Default value: 3600 Minimum value = 0 Maximum value = 2147483647
ecssubnet	<String>	Read-write	Subnet for which the cached MX record need to be removed.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
type	<String>	Read-write	Type of records to display. Available settings function as follows: * ADNS - Display all authoritative address records. * PROXY - Display all proxy address records. * ALL - Display all address records. Default value: ADNS Possible values = ALL, ADNS, PROXY
nodeid	<Integer>	Read-write	Unique number that identifies the cluster node. Minimum value = 0 Maximum value = 31
authtype	<String>	Read-only	Record type. Possible values = ALL, ADNS, PROXY
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnsmxrec **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"dnsmxrec":{

<b>"domain":<String_value>,

</b><b>"mx":<String_value>,

</b><b>"pref":<Integer_value>,

</b>"ttl":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnsmxrec/ domain_value<String> **Query-parameters: args= mx:<String_value>, ecssubnet: <String_value>**
update
URL: http:// <netscaler-ip-address> /nitro/v1/config/dnsmxrec **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"dnsmxrec":{

<b>"domain":<String_value>,
```

```
</b><b>"mx":<String_value>,

</b>"pref":<Integer_value>,

"ttl":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

unset

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnsmxrec? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"dnsmxrec":{

<b>"domain":<String_value>,

</b><b>"mx":<String_value>,

</b>"ttl":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

get (all)

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnsmxrec **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/dnsmxrec? **args=domain: <String_value> ,type: <String_value> ,nodeid: <Integer_value>**

Use this query-parameter to get dnsmxrec resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/config/dnsmxrec? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/dnsmxrec? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of dnsmxrec resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/dnsmxrec? **view=summary**

Use this query-parameter to get the summary output of dnsmxrec resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/dnsmxrec? **pagesize=#no;pageno=#no**

Use this query-parameter to get the dnsmxrec resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "dnsmxrec": [ {

domain:<String_value>,type:<String_value>,nodeid:<Integer_value>"mx":<Stri
ng_value>,

"pref":<Integer_value>,

"ttl":<Integer_value>,

"authtype":<String_value>,

"ecssubnet":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

get
URL: http:// <netscaler-ip-address> /nitro/v1/config/dnsmxrec/ domain_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/dnsmxrec/ domain_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/dnsmxrec/ domain_value<String> ? **view=summary**

Use this query-parameter to get the summary output of dnsmxrec resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "dnsmxrec": [ {

domain:<String_value>,type:<String_value>,nodeid:<Integer_value>"mx":<Stri
ng_value>,

"pref":<Integer_value>,

"ttl":<Integer_value>,

"authtype":<String_value>,

"ecssubnet":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

count
URL: http:// <netscaler-ip-address> /nitro/v1/config/dnsmxrec? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "dnsmxrec": [ { "__count": "#no"} ] }
```

dnsnameserver

Configuration for name server resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ip	<String>	Read-write	IP address of an external name server or, if the Local parameter is set, IP address of a local DNS server (LDNS). Minimum length = 1
dnsvservername	<String>	Read-write	Name of a DNS virtual server. Overrides any IP address-based name servers configured on the Citrix ADC. Minimum length = 1
local	<Boolean>	Read-write	Mark the IP address as one that belongs to a local recursive DNS server on the Citrix ADC. The appliance recursively resolves queries received on an IP address that is marked as being

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			local. For recursive resolution to work, the global DNS parameter, Recursion, must also be set. From 14.1 47.x build , it is recommended to use ADNS and ADNS_TCP service and associating a DNS profile with recursiveResolution parameter enabled to achieve the same functionality.
state	<String>	Read-write	Administrative state of the name server. Default value: ENABLED Possible values = ENABLED, DISABLED
type	<String>	Read-write	Protocol used by the name server. UDP_TCP is not valid if the name server is a DNS virtual server configured on the appliance. Default value: UDP Possible values = UDP, TCP, UDP_TCP

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
dnsprofilename	<String>	Read-write	Name of the DNS profile to be associated with the name server. Minimum length = 1
servicename	<String>	Read-only	The name of the dns vserver.
port	<Integer>	Read-only	Port of the service. Range 1 - 65535 * in CLI is represented as 65535 in NITRO API
nameserverstate	<String>	Read-only	State of the server. Possible values = UP, DOWN, UNKNOWN, BUSY, OUT OF SERVICE, GOING OUT OF SERVICE, DOWN WHEN GOING OUT OF SERVICE, NS_EMPTY_STR, Unknown, DISABLED
clmonowner	<Integer>	Read-only	Tells the mon owner of the service.
clmonview	<Integer>	Read-only	Tells the view id by which state of the service is updated.
_nextgenapiresource	<String>	Read-only	.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- UPDATE
- UNSET
- DELETE
- ENABLE
- DISABLE
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnsnameserver **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"dnsnameserver":{

"ip":<String_value>,

"dnsvservername":<String_value>,

"local":<Boolean_value>,

"state":<String_value>,

"type":<String_value>,

"dnsprofilename":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnsnameserver **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"dnsnameserver":{

<b>"ip":<String_value>,

</b>"dnsprofilename":<String_value>,

"type":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnsnameserver? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"dnsnameserver":{

<b>"ip":<String_value>,

</b>"dnsprofilename":true,

"type":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnsnameserver/ ip_value<String> **Query-parameters: args=dnsvservername: <String_value> ,type: <String_value>**
enable
URL: http:// <netscaler-ip-address> /nitro/v1/config/dnsnameserver? **action=enable HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"dnsnameserver":{

"ip":<String_value>,

"dnsvservername":<String_value>,

"type":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error
disable
URL: http:// <netscaler-ip-address> /nitro/v1/config/dnsnameserver? **action=disable HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"dnsnameserver":{

"ip":<String_value>,

"dnsvservername":<String_value>,

"type":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error
get (all)
URL: http:// <netscaler-ip-address> /nitro/v1/config/dnsnameserver **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/dnsnameserver? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/dnsnameserver? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of dnsnameserver resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/dnsnameserver? **view=summary**

Use this query-parameter to get the summary output of dnsnameserver resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/dnsnameserver? **pagesize=#no;pageno=#no**

Use this query-parameter to get the dnsnameserver resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "dnsnameserver": [ {

"ip":<String_value>,

"dnsvservername":<String_value>,

"servicename":<String_value>,

"port":<Integer_value>,

"type":<String_value>,

"state":<String_value>,

"nameserverstate":<String_value>,

"local":<Boolean_value>,

"clmonowner":<Integer_value>,

"clmonview":<Integer_value>,

"dnsprofilename":<String_value>,

"_nextgenapiresource":<String_value>
```

```
}]}
```

count

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnsnameserver? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "dnsnameserver": [ { "__count": "#no"} ] }
```

dnsnaptrrec

Configuration for NAPTR record resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
domain	<String>	Read-write	Name of the domain for the NAPTR record. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
order	<Integer>	Read-write	An integer specifying the order in which the NAPTR records MUST be processed in order to accurately represent the ordered list of Rules. The ordering is from lowest to highest. Minimum value = 0 Maximum value = 65535
preference	<Integer>	Read-write	An integer specifying the preference of this NAPTR among NAPTR records having same order. lower the number, higher the preference. Minimum value = 0 Maximum value = 65535
flags	<String>	Read-write	flags for this NAPTR. Maximum length = 255
services	<String>	Read-write	Service Parameters applicable to this delegation path. Maximum length = 255
regexp	<String>	Read-write	The regular expression, that specifies the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			substitution expression for this NAPTR. Maximum length = 255
replacement	<String>	Read-write	The replacement domain name for this NAPTR. Maximum length = 255
ttl	<Integer>	Read-write	Time to Live (TTL), in seconds, for the record. TTL is the time for which the record must be cached by DNS proxies. The specified TTL is applied to all the resource records that are of the same record type and belong to the specified domain name. For example, if you add an address record, with a TTL of 36000, to the domain name example.com, the TTLs of all the address records of example.com are changed to 36000. If the TTL is not specified, the Citrix ADC uses either the DNS zone's minimum TTL or, if

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			the SOA record is not available on the appliance, the default value of 3600. Default value: 3600 Minimum value = 0 Maximum value = 2147483647
recordid	<Integer>	Read-write	Unique, internally generated record ID. View the details of the naptr record to obtain its record ID. Records can be removed by either specifying the domain name and record id OR by specifying domain name and all other naptr record attributes as was supplied during the add command. Minimum value = 1 Maximum value = 65535
ecssubnet	<String>	Read-write	Subnet for which the cached NAPTR record need to be removed.
type	<String>	Read-write	Type of records to display. Available

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			settings function as follows: * ADNS - Display all authoritative address records. * PROXY - Display all proxy address records. * ALL - Display all address records. Default value: ADNS Possible values = ALL, ADNS, PROXY
nodeid	<Integer>	Read-write	Unique number that identifies the cluster node. Minimum value = 0 Maximum value = 31
authtype	<String>	Read-only	Authentication type. Possible values = ALL, ADNS, PROXY
vservername	<String>	Read-only	Virtual server name.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnsnaptrrec **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"dnsnaptrrec":{

<b>"domain":<String_value>,

</b><b>"order":<Integer_value>,

</b><b>"preference":<Integer_value>,

</b>"flags":<String_value>,

"services":<String_value>,

"regexp":<String_value>,

"replacement":<String_value>,

"ttl":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnsnaptrrec/ domain_value<String> **Query-parameters: args=order: <Integer_value> ,recordid: <Integer_value> ,ecssubnet: <String_value> ,preference: <Integer_value> ,flags: <String_value> ,services: <String_value> ,regexp: <String_value> ,replacement: <String_value>**
get (all)
URL: http:// <netscaler-ip-address> /nitro/v1/config/dnsnaptrrec **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/dnsnaptrrec? **args=domain: <String_value> ,type: <String_value> ,nodeid: <Integer_value>**

Use this query-parameter to get dnsnaptrrec resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/config/dnsnaptrrec? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/dnsnaptrrec? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of dnsnaptrrec resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/dnsnaptrrec? **view=summary**

Use this query-parameter to get the summary output of dnsnaptrrec resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/dnsnaptrrec? **pagesize=#no;pageno=#no**

Use this query-parameter to get the dnsnaptrrec resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "dnsnaptrrec": [ {

domain:<String_value>,type:<String_value>,nodeid:<Integer_value>"order":<I
nteger_value>,

"preference":<Integer_value>,

"flags":<String_value>,

"services":<String_value>,

"regexp":<String_value>,

"replacement":<String_value>,

"ttl":<Integer_value>,

"recordid":<Integer_value>,

"authtype":<String_value>,

"ecssubnet":<String_value>,

"vservername":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

get

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnsnaptrrec/ domain_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/dnsnaptrrec/ domain_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/dnsnaptrrec/ domain_value<String> ? **view=summary**

Use this query-parameter to get the summary output of dnsnaptrrec resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "dnsnaptrrec": [ {

domain:<String_value>,type:<String_value>,nodeid:<Integer_value>"order":<I
nteger_value>,

"preference":<Integer_value>,

"flags":<String_value>,

"services":<String_value>,

"regexp":<String_value>,

"replacement":<String_value>,

"ttl":<Integer_value>,

"recordid":<Integer_value>,

"authtype":<String_value>,

"ecssubnet":<String_value>,
```

```
"vservername":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

count

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnsnaptrrec? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "dnsnaptrrec": [ { "__count": "#no"} ] }
```

dnsnegativecacherecords

Configuration for Negative Cache Records resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
nodeid	<Integer>	Read-write	Unique number that identifies the cluster node.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum value = 0 Maximum value = 31
hostname	<String>	Read-only	Domain name. Minimum length = 1
negcachetype	<String>	Read-only	negative cache record type. Possible values = NODATA, NXDOMAIN, CNAME-REFERRAL
rdclient	<String>	Read-only	cname referral type. Possible values = YES, NO, NA
querytype	<String>	Read-only	DNS query type. Possible values = A, NS, CNAME, SOA, MX, AAAA, SRV, RRSIG, NSEC, DNSKEY, PTR, TXT, NAPTR, CAA, SVCB, HTTPS
ttl	<Integer>	Read-only	Time to Live (TTL), in seconds, for the record. Default value: 3600 Minimum value = 0 Maximum value = 2147483647

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ecssubnet	<String>	Read-only	Subnet for which this particular record is cached. Subnet caching will occur for responses with EDNS Client Subnet (ECS) option. Applies to resource records obtained through proxy configurations only.
peid	<Integer>	Read-only	PE where the cache is stored. Minimum value = 0 Maximum value = 32
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnsnegativecacherecords **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/dnsnegativecacherecords? **args=nodeid: <Integer_value>**

Use this query-parameter to get dnsnegativecacherecords resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/config/dnsnegativecacherecords? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/dnsnegativecacherecords? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of dnsnegativecacherecords resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/dnsnegativecacherecords? **view=summary**

Use this query-parameter to get the summary output of dnsnegativecacherecords resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/dnsnegativecacherecords? **pagesize=#no;pageno=#no**

Use this query-parameter to get the dnsnegativecacherecords resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "dnsnegativecacherecords": [ {

nodeid:<Integer_value>"hostname":<String_value>,

"negcachetype":<String_value>,

"rdclient":<String_value>,

"querytype":<String_value>,

"ttl":<Integer_value>,

"ecssubnet":<String_value>,

"peid":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnsnegativecacherecords? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "dnsnegativecacherecords": [ { "__count": "#no"} ] }
```

dnsnsecrec

Configuration for 0 resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
hostname	<String>	Read-write	Name of the domain. Minimum length = 1
type	<String>	Read-write	Type of records to display. Available settings function as follows:

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			* ADNS - Display all authoritative address records. * PROXY - Display all proxy address records. * ALL - Display all address records. Possible values = ALL, ADNS, PROXY
nextnsec	<String>	Read-only	Next nsec record in the chain.
nextrecs	<String[]>	Read-only	An array of record types associated with the nsec record. Possible values = A, NS, CNAME, SOA, MX, AAAA, SRV, RRSIG, NSEC, DNSKEY, PTR, TXT, NAPTR, CAA, SVCB, HTTPS
ttl	<Integer>	Read-only	Time to Live (TTL), in seconds, for the record.
ecssubnet	<String>	Read-only	Subnet for which this particular record is cached. Subnet caching will occur for responses with EDNS Client Subnet (ECS) option.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Applies to resource records obtained through proxy configurations only.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnsnsecrec **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/dnsnsecrec? **args=hostname: <String_value> ,type: <String_value>**

Use this query-parameter to get dnsnsecrec resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/config/dnsnsecrec? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/dnsnsecrec? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of dnsnsecrec resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/dnsnsecrec? **view=summary**

Use this query-parameter to get the summary output of dnsnsecrec resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/dnsnsecrec? **pagesize=#no;pageno=#no**

Use this query-parameter to get the dnsnsecrec resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "dnsnsecrec": [ {

hostname:<String_value>,type:<String_value>"nextnsec":<String_value>,

"nsecbitarray":<String[]_value>,

"nextrecs":<String[]_value>,

"ttl":<Integer_value>,

"ecssubnet":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnsnsecrec/ hostname_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/dnsnsecrec/ hostname_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/dnsnsecrec/ hostname_value<String> ? **view=summary**

Use this query-parameter to get the summary output of dnsnsecrec resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "dnsnsecrec": [ {

hostname:<String_value>,type:<String_value>"nextnsec":<String_value>,

"nsecbitarray":<String[]_value>,

"nextrecs":<String[]_value>,

"ttl":<Integer_value>,

"ecssubnet":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnsnsecrec? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "dnsnsecrec": [ { "__count": "#no"} ] }
```

dnsnsrec

Configuration for name server record resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
domain	<String>	Read-write	Domain name. Minimum length = 1
nameserver	<String>	Read-write	Host name of the name server to add to the domain. Minimum length = 1
ttl	<Integer>	Read-write	Time to Live (TTL), in seconds, for the record. TTL is the time for which the record must be cached by DNS proxies. The specified TTL is applied to all the resource records that are of the same record type and belong to the specified domain

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			name. For example, if you add an address record, with a TTL of 36000, to the domain name example.com, the TTLs of all the address records of example.com are changed to 36000. If the TTL is not specified, the Citrix ADC uses either the DNS zone's minimum TTL or, if the SOA record is not available on the appliance, the default value of 3600. Default value: 3600 Minimum value = 0 Maximum value = 2147483647
ecssubnet	<String>	Read-write	Subnet for which the cached name server record need to be removed.
type	<String>	Read-write	Type of records to display. Available settings function as follows: * ADNS - Display all authoritative address records.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			* PROXY - Display all proxy address records. * ALL - Display all address records. Possible values = ALL, ADNS, PROXY
nodeid	<Integer>	Read-write	Unique number that identifies the cluster node. Minimum value = 0 Maximum value = 31
authtype	<String>	Read-only	Record type. Possible values = ALL, ADNS, PROXY
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnsnsrec **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"dnsnsrec":{

<b>"domain":<String_value>,

</b><b>"nameserver":<String_value>,

</b>"ttl":<Integer_value>
```

```
}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnsnsrec/ domain_value<String> **Query-parameters: args= nameserver:<String_value>, ecssubnet: <String_value>**
get (all)
URL: http:// <netscaler-ip-address> /nitro/v1/config/dnsnsrec **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/dnsnsrec? **args=domain: <String_value> ,type: <String_value> ,nodeid: <Integer_value>**

Use this query-parameter to get dnsnsrec resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/config/dnsnsrec? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/dnsnsrec? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of dnsnsrec resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/dnsnsrec? **view=summary**

Use this query-parameter to get the summary output of dnsnsrec resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/dnsnsrec? **pagesize=#no;pageno=#no**

Use this query-parameter to get the dnsnsrec resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "dnsnsrec": [ {

domain:<String_value>,type:<String_value>,nodeid:<Integer_value>"nameserve
r":<String_value>,

"ecssubnet":<String_value>,

"ttl":<Integer_value>,

"authtype":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

get
URL: http:// <netscaler-ip-address> /nitro/v1/config/dnsnsrec/ domain_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/dnsnsrec/ domain_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/dnsnsrec/ domain_value<String> ? **view=summary**

Use this query-parameter to get the summary output of dnsnsrec resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "dnsnsrec": [ {

domain:<String_value>,type:<String_value>,nodeid:<Integer_value>"nameserve
r":<String_value>,

"ecssubnet":<String_value>,

"ttl":<Integer_value>,

"authtype":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

count
URL: http:// <netscaler-ip-address> /nitro/v1/config/dnsnsrec? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "dnsnsrec": [ { "__count": "#no"} ] }
```

dnsparameter

Configuration for DNS parameter resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
retries	<Integer>	Read-write	Maximum number of retry attempts when no response is received for a query sent to a name server. Applies to end resolver and forwarder configurations. Default value: 5 Minimum value = 1 Maximum value = 5
minttl	<Integer>	Read-write	Minimum permissible time to live (TTL) for all records cached in

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			the DNS cache by DNS proxy, end resolver, and forwarder configurations. If the TTL of a record that is to be cached is lower than the value configured for minTTL, the TTL of the record is set to the value of minTTL before caching. When you modify this setting, the new value is applied only to those records that are cached after the modification. The TTL values of existing records are not changed. Minimum value = 0 Maximum value = 604800
maxttl	<Integer>	Read-write	Maximum time to live (TTL) for all records cached in the DNS cache by DNS proxy, end resolver, and forwarder configurations. If the TTL of a record that is to be cached is higher than the value configured for maxTTL, the TTL of the record is set to the value of maxTTL

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			before caching. When you modify this setting, the new value is applied only to those records that are cached after the modification. The TTL values of existing records are not changed. Default value: 604800 Minimum value = 1 Maximum value = 604800
cacherecords	<String>	Read-write	Cache resource records in the DNS cache. Applies to resource records obtained through proxy configurations only. End resolver and forwarder configurations always cache records in the DNS cache, and you cannot disable this behavior. When you disable record caching, the appliance stops caching server responses. However, cached records are not flushed. The appliance does not serve requests from

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			the cache until record caching is enabled again. Default value: YES Possible values = YES, NO
namelookuppriority	<String>	Read-write	Type of lookup (DNS or WINS) to attempt first. If the first-priority lookup fails, the second-priority lookup is attempted. Used only by the SSL VPN feature. Default value: WINS Possible values = WINS, DNS
recursion	<String>	Read-write	Function as an end resolver and recursively resolve queries for domains that are not hosted on the Citrix ADC. Also resolve queries recursively when the external name servers configured on the appliance (for a forwarder configuration) are unavailable. When external name servers are unavailable, the appliance queries a root server and resolves the request

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			recursively, as it does for an end resolver configuration. This parameter will be effective only for queries recieved on nameserver with local flag. To enable recursion for queries recieved through ADNS service , CS vserver and LB vserver it is recommended to use recursiveResolution parameter on DNS profile. Default value: DISABLED Possible values = ENABLED, DISABLED
resolutionorder	<String>	Read-write	Type of DNS queries (A, AAAA, or both) to generate during the routine functioning of certain Citrix ADC features, such as SSL VPN, cache redirection, and the integrated cache. The queries are sent to the external name servers that are configured for the forwarder function. If you specify both query types, you can

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			also specify the order. Available settings function as follows: * OnlyAQuery. Send queries for IPv4 address records (A records) only. * OnlyAAAAQuery. Send queries for IPv6 address records (AAAA records) instead of queries for IPv4 address records (A records). * AThenAAAAQuery. Send a query for an A record, and then send a query for an AAAA record if the query for the A record results in a NODATA response from the name server. * AAAAThenAQuery. Send a query for an AAAA record, and then send a query for an A record if the query for the AAAA record results in a

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			NODATA response from the name server. Default value: OnlyAQuery Possible values = OnlyAQuery, OnlyAAAAQuery, AThenAAAAQuery, AAAAThenAQuery
dnssec	<String>	Read-write	Enable or disable the Domain Name System Security Extensions (DNSSEC) feature on the appliance. Note: Even when the DNSSEC feature is enabled, forwarder configurations (used by internal Citrix ADC features such as SSL VPN and Cache Redirection for name resolution) do not support the DNSSEC OK (DO) bit in the EDNS0 OPT header. Default value: ENABLED Possible values = ENABLED, DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
maxpipeline	<Integer>	Read-write	Maximum number of concurrent DNS requests to allow on a single client connection, which is identified by the <clientip:port>-<vserver ip:port> tuple. A value of 0 (zero) applies no limit to the number of concurrent DNS requests allowed on a single client connection.
dnsrootreferral	<String>	Read-write	Send a root referral if a client queries a domain name that is unrelated to the domains configured/cached on the Citrix ADC. If the setting is disabled, the appliance sends a blank response instead of a root referral. Applicable to domains for which the appliance is authoritative. Disable the parameter when the appliance is under attack from a client that is sending a flood of queries for unrelated domains. Default value: DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ENABLED, DISABLED
dns64timeout	<Integer>	Read-write	While doing DNS64 resolution, this parameter specifies the time to wait before sending an A query if no response is received from backend DNS server for AAAA query. Minimum value = 0 Maximum value = 10000
ecsmaxsubnets	<Integer>	Read-write	Maximum number of subnets that can be cached corresponding to a single domain. Subnet caching will occur for responses with EDNS Client Subnet (ECS) option. Caching of such responses can be disabled using DNS profile settings. A value of zero indicates that the number of subnets cached is limited only by existing memory constraints. The default value is zero.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: 0 Minimum value = 0 Maximum value = 1280
maxnegcachettl	<Integer>	Read-write	Maximum time to live (TTL) for all negative records (NXDONAIN and NODATA) cached in the DNS cache by DNS proxy, end resolver, and forwarder configurations. If the TTL of a record that is to be cached is higher than the value configured for maxnegcacheTTL, the TTL of the record is set to the value of maxnegcacheTTL before caching. When you modify this setting, the new value is applied only to those records that are cached after the modification. The TTL values of existing records are not changed. Default value: 604800 Minimum value = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum value = 604800
cachehitbypass	<String>	Read-write	This parameter is applicable only in proxy mode and if this parameter is enabled we will forward all the client requests to the backend DNS server and the response served will be cached on Citrix ADC. Default value: DISABLED Possible values = ENABLED, DISABLED
maxcachesize	<Integer>	Read-write	Maximum memory, in megabytes, that can be used for dns caching per Packet Engine.
resolvermaxactiveresolutions	<Integer>	Read-write	Maximum number of active concurrent DNS resolutions per Packet Engine. Default value: 0
resolvermaxtcpconnections	<Integer>	Read-write	Maximum DNS-TCP connections opened for recursive resolution per Packet Engine.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: 1000 Minimum value = 1
resolvermaxtcptimeout	<Integer>	Read-write	Maximum wait time in seconds for the response on DNS-TCP connection for recursive resolution per Packet Engine. Default value: 5 Minimum value = 1 Maximum value = 120
maxnegativecachesize	<Integer>	Read-write	Maximum memory, in megabytes, that can be used for caching of negative DNS responses per packet engine.
cachenoexpire	<String>	Read-write	If this flag is set to YES, the existing entries in cache do not age out. On reaching the max limit the cache records are frozen. Default value: DISABLED Possible values = ENABLED, DISABLED
splitpktqueryprocessing	<String>	Read-write	Processing requests split across multiple packets.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: ALLOW Possible values = ALLOW, DROP
cacheecszeroprefix	<String>	Read-write	Cache ECS responses with a Scope Prefix length of zero. Such a cached response will be used for all queries with this domain name and any subnet. When disabled, ECS responses with Scope Prefix length of zero will be cached, but not tied to any subnet. This option has no effect if caching of ECS responses is disabled in the corresponding DNS profile. Default value: ENABLED Possible values = ENABLED, DISABLED
maxudppacketsize	<Integer>	Read-write	Maximum UDP packet size that can be handled by Citrix ADC. This is the value advertised by Citrix ADC when responding as an

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			authoritative server and it is also used when Citrix ADC queries other name servers as a forwarder. When acting as a proxy, requests from clients are limited by this parameter - if a request contains a size greater than this value in the OPT record, it will be replaced. Default value: 1280 Minimum value = 512 Maximum value = 16384
zonetransfer	<String>	Read-write	Flag to enable/ disable DNS zones configuration transfer to remote GSLB site nodes. Default value: DISABLED Possible values = ENABLED, DISABLED
autosavekeyops	<String>	Read-write	Flag to enable/ disable saving of rollover operations executed

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			automatically to avoid config loss. Applicable only when autorollover option is enabled on a key. Note: when you enable this, full configuration will be saved. Default value: DISABLED Possible values = ENABLED, DISABLED
nxdomainratelimitthreshold	<Integer>	Read-write	Rate limit threshold for Non-Existant domain (NXDOMAIN) responses generated from Citrix ADC. Once the threshold is breached , DNS queries leading to NXDOMAIN response will be dropped. This threshold will not be applied for NXDOMAIN responses got from the backend. The threshold will be applied per packet engine and per second.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
builtin	<String[]>	Read-only	Flag to determine if dns param is built-in or not. Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL
feature	<String>	Read-only	The feature to be checked while applying this config.
nxdomainthresholdcrossed	<Integer>	Read-only	Number of times requests has been dropped as number of DNS queries leading to NXDOMAIN response has crossed the threshold.
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- UPDATE
- UNSET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnsparameter **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"dnsparameter":{

"retries":<Integer_value>,

"minttl":<Integer_value>,

"maxttl":<Integer_value>,

"cacherecords":<String_value>,

"namelookuppriority":<String_value>,

"recursion":<String_value>,
```

```
"resolutionorder":<String_value>,

"dnssec":<String_value>,

"maxpipeline":<Integer_value>,

"dnsrootreferral":<String_value>,

"dns64timeout":<Integer_value>,

"ecsmaxsubnets":<Integer_value>,

"maxnegcachettl":<Integer_value>,

"cachehitbypass":<String_value>,

"maxcachesize":<Integer_value>,

"resolvermaxactiveresolutions":<Integer_value>,

"resolvermaxtcpconnections":<Integer_value>,

"resolvermaxtcptimeout":<Integer_value>,

"maxnegativecachesize":<Integer_value>,

"cachenoexpire":<String_value>,

"splitpktqueryprocessing":<String_value>,

"cacheecszeroprefix":<String_value>,

"maxudppacketsize":<Integer_value>,

"zonetransfer":<String_value>,

"autosavekeyops":<String_value>,

"nxdomainratelimitthreshold":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnsparameter? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"dnsparameter":{

"retries":true,

"minttl":true,

"maxttl":true,

"cacherecords":true,

"namelookuppriority":true,

"recursion":true,

"resolutionorder":true,

"dnssec":true,

"maxpipeline":true,

"dnsrootreferral":true,

"dns64timeout":true,
```

```
"ecsmaxsubnets":true,

"maxnegcachettl":true,

"cachehitbypass":true,

"maxcachesize":true,

"resolvermaxactiveresolutions":true,

"resolvermaxtcpconnections":true,

"resolvermaxtcptimeout":true,

"maxnegativecachesize":true,

"cachenoexpire":true,

"splitpktqueryprocessing":true,

"cacheecszeroprefix":true,

"maxudppacketsize":true,

"zonetransfer":true,

"autosavekeyops":true,

"nxdomainratelimitthreshold":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnsparameter **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "dnsparameter": [ {

"retries":<Integer_value>,

"minttl":<Integer_value>,

"maxttl":<Integer_value>,

"namelookuppriority":<String_value>,

"cacherecords":<String_value>,

"recursion":<String_value>,

"resolutionorder":<String_value>,

"dnssec":<String_value>,

"maxpipeline":<Integer_value>,

"dnsrootreferral":<String_value>,

"dns64timeout":<Integer_value>,

"ecsmaxsubnets":<Integer_value>,

"maxnegcachettl":<Integer_value>,

"cachehitbypass":<String_value>,
```

```
"maxcachesize":<Integer_value>,

"resolvermaxactiveresolutions":<Integer_value>,

"resolvermaxtcpconnections":<Integer_value>,

"resolvermaxtcptimeout":<Integer_value>,

"maxnegativecachesize":<Integer_value>,

"cachenoexpire":<String_value>,

"splitpktqueryprocessing":<String_value>,

"cacheecszeroprefix":<String_value>,

"maxudppacketsize":<Integer_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"nxdomainratelimitthreshold":<Integer_value>,

"zonetransfer":<String_value>,

"autosavekeyops":<String_value>,

"nxdomainthresholdcrossed":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

dnspolicy

Configuration for DNS policy resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the DNS policy.
rule	<String>	Read-write	Expression against which DNS traffic is evaluated. Note: * On the command line interface, if the expression includes blank spaces, the entire expression must be enclosed in double quotation marks. * If the expression itself includes double quotation marks, you must escape the quotations by using the character. * Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks. Example: CLIENT.UDP.DNS.DOMAIN.EQ("domainname").

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
viewname	<String>	Read-write	The view name that must be used for the given policy.
preferredlocation	<String>	Read-write	The location used for the given policy. This is deprecated attribute. Please use -prefLocList.
preferredloclist	<String[]>	Read-write	The location list in priority order used for the given policy. Minimum length = 1
drop	<String>	Read-write	The dns packet must be dropped. Possible values = YES, NO
cachebypass	<String>	Read-write	By pass dns cache for this. Possible values = YES, NO
actionname	<String>	Read-write	Name of the DNS action to perform when the rule evaluates to TRUE. The built in actions function as follows: * dns_default_act_Drop. Drop the DNS request. * dns_default_act_Cachebypass. Bypass the DNS cache and

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			forward the request to the name server. You can create custom actions by using the add dns action command in the CLI or the DNS > Actions > Create DNS Action dialog box in the Citrix ADC configuration utility.
logaction	<String>	Read-write	Name of the messagelog action to use for requests that match this policy.
hits	<Integer>	Read-only	The number of times the policy has been hit.
undefhits	<Integer>	Read-only	Number of Undef hits.
description	<String>	Read-only	Description of the policy.
builtin	<String[]>	Read-only	Flag to determine whether DNS policy is default or not. Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
feature	<String>	Read-only	The feature to be checked while applying this config.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnspolicy **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"dnspolicy":{

<b>"name":<String_value>,

</b><b>"rule":<String_value>,

</b>"viewname":<String_value>,

"preferredlocation":<String_value>,

"preferredloclist":<String[]_value>,

"drop":<String_value>,

"cachebypass":<String_value>,

"actionname":<String_value>,

"logaction":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnspolicy/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnspolicy **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"dnspolicy":{

<b>"name":<String_value>,

</b>"rule":<String_value>,

"viewname":<String_value>,

"preferredlocation":<String_value>,

"preferredloclist":<String[]_value>,

"drop":<String_value>,

"cachebypass":<String_value>,
```

```
"actionname":<String_value>,

"logaction":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnspolicy? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"dnspolicy":{

<b>"name":<String_value>,

</b>"logaction":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnspolicy **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/dnspolicy? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/dnspolicy? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of dnspolicy resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/dnspolicy? **view=summary**

Use this query-parameter to get the summary output of dnspolicy resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/dnspolicy? **pagesize=#no;pageno=#no**

Use this query-parameter to get the dnspolicy resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "dnspolicy": [ {

"name":<String_value>,

"rule":<String_value>,

"viewname":<String_value>,
```

```
"preferredlocation":<String_value>,

"preferredloclist":<String[]_value>,

"hits":<Integer_value>,

"undefhits":<Integer_value>,

"drop":<String_value>,

"actionname":<String_value>,

"cachebypass":<String_value>,

"description":<String_value>,

"logaction":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnspolicy/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/dnspolicy/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/dnspolicy/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of dnspolicy resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "dnspolicy": [ {

"name":<String_value>,

"rule":<String_value>,

"viewname":<String_value>,

"preferredlocation":<String_value>,

"preferredloclist":<String[]_value>,

"hits":<Integer_value>,

"undefhits":<Integer_value>,

"drop":<String_value>,

"actionname":<String_value>,

"cachebypass":<String_value>,

"description":<String_value>,

"logaction":<String_value>,
```

```
"builtin":<String[]_value>,

"feature":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnspolicy? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "dnspolicy": [ { "__count": "#no"} ] }
```

dnspolicy64

Configuration for dns64 policy resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the DNS64 policy.
rule	<String>	Read-write	Expression against which DNS traffic is evaluated. Note: * On the command line interface, if the expression includes blank spaces, the entire expression must be enclosed in double quotation marks. * If the expression itself includes double quotation marks, you must escape the quotations by using the character. * Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks. Example: CLIENT.IP.SRC.IN_SUBENT(23.34.0.0/16).

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
action	<String>	Read-write	Name of the DNS64 action to perform when the rule evaluates to TRUE. The built in actions function as follows: * A default dns64 action with prefix <default prefix> and mapped and exclude are any You can create custom actions by using the add dns action command in the CLI or the DNS64 > Actions > Create DNS64 Action dialog box in the Citrix ADC configuration utility.
hits	<Integer>	Read-only	The number of times the policy has been hit.
labeltype	<String>	Read-only	Type of policy label invocation. Possible values = reqvserver, resvserver, policylabel
labelname	<String>	Read-only	Name of the label to invoke if the current policy rule evaluates to TRUE.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
undefhits	<Integer>	Read-only	Number of Undef hits.
description	<String>	Read-only	Description of the policy.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnspolicy64 **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"dnspolicy64":{

<b>"name":<String_value>,

</b><b>"rule":<String_value>,

</b>"action":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnspolicy64/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnspolicy64 **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"dnspolicy64":{

<b>"name":<String_value>,

</b>"rule":<String_value>,

"action":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnspolicy64 **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/dnspolicy64? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/dnspolicy64? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of dnspolicy64 resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/dnspolicy64? **view=summary**

Use this query-parameter to get the summary output of dnspolicy64 resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/dnspolicy64? **pagesize=#no;pageno=#no**

Use this query-parameter to get the dnspolicy64 resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "dnspolicy64": [ {

"name":<String_value>,

"rule":<String_value>,

"hits":<Integer_value>,

"action":<String_value>,

"labeltype":<String_value>,

"labelname":<String_value>,
```

```
"undefhits":<Integer_value>,

"description":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnspolicy64/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/dnspolicy64/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/dnspolicy64/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of dnspolicy64 resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "dnspolicy64": [ {

"name":<String_value>,

"rule":<String_value>,

"hits":<Integer_value>,

"action":<String_value>,

"labeltype":<String_value>,

"labelname":<String_value>,

"undefhits":<Integer_value>,

"description":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnspolicy64? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "dnspolicy64": [ { "__count": "#no"} ] }
```

dnspolicy64_binding

Binding object which returns the resources bound to dnspolicy64.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the DNS64 policy.
dnspolicy64_lbvserver_binding	<dnspolicy64_lbvserver_binding[]>	Read-only	lbvserver that can be bound to dnspolicy64.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.
- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnspolicy64_binding/ name_value<String>

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "dnspolicy64_binding": [ {

"name":<String_value>,

"dnspolicy64_lbvserver_binding":<dnspolicy64_lbvserver_binding[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnspolicy64_binding

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters:

bulkbindings

http:// <netscaler-ip-address> /nitro/v1/config/dnspolicy64_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "dnspolicy64_binding": [ {

"name":<String_value>,

"dnspolicy64_lbvserver_binding":<dnspolicy64_lbvserver_binding[]_value>

}]}
```

dnspolicy64_lbvserver_binding

Binding object showing the lbvserver that can be bound to dnspolicy64.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
boundto	<String>	Read-write	Location where policy is bound.
name	<String>	Read-write	Name of the DNS64 policy.
gotopriorityexpression	<String>	Read-only	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
priority	<Integer>	Read-only	Specifies the priority of the policy.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnspolicy64_lbvserver_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ dnspolicy64_lbvserver_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of dnspolicy64_lbvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/dnspolicy64_lbvserver_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the dnspolicy64_lbvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "dnspolicy64_lbvserver_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"gotopriorityexpression":<String_value>,

"priority":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnspolicy64_lbvserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/dnspolicy64_lbvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "dnspolicy64_lbvserver_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"gotopriorityexpression":<String_value>,

"priority":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnspolicy64_lbvserver_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"dnspolicy64_lbvserver_binding": [ { "__count": "#no"} ] }
```

dnspolicy_binding

Binding object which returns the resources bound to dnspolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the DNS policy.
dnspolicy_dnspolicylabel_binding	<dnspolicy_dnspolicylabel_binding[]>	Read-only	dnspolicylabel that can be bound to dnspolicy.
dnspolicy_dnsglobal_binding	<dnspolicy_dnsglobal_binding[]>	Read-only	dnsglobal that can be bound to dnspolicy.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnspolicy_binding/ name_value<String>

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "dnspolicy_binding": [ {

"name":<String_value>,
```

```
"dnspolicy_dnspolicylabel_binding":<dnspolicy_dnspolicylabel_binding[]_val
ue>,

"dnspolicy_dnsglobal_binding":<dnspolicy_dnsglobal_binding[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnspolicy_binding

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters:

bulkbindings

http:// <netscaler-ip-address> /nitro/v1/config/dnspolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "dnspolicy_binding": [ {

"name":<String_value>,

"dnspolicy_dnspolicylabel_binding":<dnspolicy_dnspolicylabel_binding[]_value>,

"dnspolicy_dnsglobal_binding":<dnspolicy_dnsglobal_binding[]_value>

}]}
```

dnspolicy_dnsglobal_binding

Binding object showing the dnsglobal that can be bound to dnspolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
boundto	<String>	Read-write	Location where policy is bound.
name	<String>	Read-write	Name of the DNS policy.
priority	<Integer>	Read-only	Specifies the priority of the policy.
labeltype	<String>	Read-only	Type of policy label invocation. Possible values = reqvserver, resvserver, policylabel
activepolicy	<Integer>	Read-only	Indicates whether policy is bound or not.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
gotopriorityexpression	<String>	Read-only	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
labelname	<String>	Read-only	Name of the label to invoke if the current policy rule evaluates to TRUE.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnspolicy_dnsglobal_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ dnspolicy_dnsglobal_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of dnspolicy_dnsglobal_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/dnspolicy_dnsglobal_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the dnspolicy_dnsglobal_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "dnspolicy_dnsglobal_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"priority":<Integer_value>,

"labeltype":<String_value>,

"activepolicy":<Integer_value>,

"gotopriorityexpression":<String_value>,

"labelname":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnspolicy_dnsglobal_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/dnspolicy_dnsglobal_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "dnspolicy_dnsglobal_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"priority":<Integer_value>,

"labeltype":<String_value>,

"activepolicy":<Integer_value>,

"gotopriorityexpression":<String_value>,

"labelname":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnspolicy_dnsglobal_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"dnspolicy_dnsglobal_binding": [ { "__count": "#no"} ] }
```

dnspolicy_dnspolicylabel_binding

Binding object showing the dnspolicylabel that can be bound to dnspolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the DNS policy.
boundto	<String>	Read-write	Location where policy is bound.
labelname	<String>	Read-only	Name of the label to invoke if the current policy rule evaluates to TRUE.
gotopriorityexpression	<String>	Read-only	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
activepolicy	<Integer>	Read-only	Indicates whether policy is bound or not.
labeltype	<String>	Read-only	Type of policy label invocation. Possible values = reqvserver, resvserver, policylabel

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
priority	<Integer>	Read-only	Specifies the priority of the policy.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnspolicy_dnspolicylabel_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ dnspolicy_dnspolicylabel_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of dnspolicy_dnspolicylabel_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/dnspolicy_dnspolicylabel_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the dnspolicy_dnspolicylabel_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "dnspolicy_dnspolicylabel_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"labelname":<String_value>,

"gotopriorityexpression":<String_value>,

"activepolicy":<Integer_value>,
```

```
"labeltype":<String_value>,

"priority":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnspolicy_dnspolicylabel_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/dnspolicy_dnspolicylabel_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "dnspolicy_dnspolicylabel_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"labelname":<String_value>,
```

```
"gotopriorityexpression":<String_value>,

"activepolicy":<Integer_value>,

"labeltype":<String_value>,

"priority":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnspolicy_dnspolicylabel_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"dnspolicy_dnspolicylabel_binding": [ { "__count": "#no"} ] }
```

dnspolicylabel

Configuration for dns policy label resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
labelname	<String>	Read-write	Name of the dns policy label.
transform	<String>	Read-write	The type of transformations allowed by the policies bound to the label. Possible values = dns_req, dns_res
newname	<String>	Read-write	The new name of the dns policylabel. Minimum length = 1
numpol	<Integer>	Read-only	Number of polices bound to label.
hits	<Integer>	Read-only	Number of times policy label was invoked.
priority	<Integer>	Read-only	Specifies the priority of the policy.
gotopriorityexpression	<String>	Read-only	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
labeltype	<String>	Read-only	Type of policy label invocation. Possible values = policylabel
invoke_labelname	<String>	Read-only	Name of the label to invoke if the current

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			policy rule evaluates to TRUE.
flowtype	<Integer>	Read-only	Flowtype of the bound dns policy.
description	<String>	Read-only	Description of the policylabel.
isdefault	<Boolean>	Read-only	A value of true is returned if it is a default dns policylabel.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET (ALL)
- GET
- COUNT
- RENAME

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnspolicylabel **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"dnspolicylabel":{

<b>"labelname":<String_value>,

</b><b>"transform":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnspolicylabel/ labelname_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

RENAME

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnspolicylabel? **action=rename HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"dnspolicylabel":{

<b>"labelname":<String_value>,

</b><b>"newname":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnspolicylabel **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/dnspolicylabel? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/dnspolicylabel? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of dnspolicylabel resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/dnspolicylabel? **view=summary**

Use this query-parameter to get the summary output of dnspolicylabel resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/dnspolicylabel? **pagesize=#no;pageno=#no**

Use this query-parameter to get the dnspolicylabel resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "dnspolicylabel": [ {

"labelname":<String_value>,

"transform":<String_value>,
```

```
"numpol":<Integer_value>,

"hits":<Integer_value>,

"priority":<Integer_value>,

"gotopriorityexpression":<String_value>,

"labeltype":<String_value>,

"invoke_labelname":<String_value>,

"flowtype":<Integer_value>,

"description":<String_value>,

"isdefault":<Boolean_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnspolicylabel/ labelname_value<String>
Query-parameters: attrs http:// <netscaler-ip-address> /nitro/v1/config/dnspolicylabel/ labelname_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/dnspolicylabel/ labelname_value<String> ? **view=summary**

Use this query-parameter to get the summary output of dnspolicylabel resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "dnspolicylabel": [ {

"labelname":<String_value>,

"transform":<String_value>,

"numpol":<Integer_value>,

"hits":<Integer_value>,

"priority":<Integer_value>,

"gotopriorityexpression":<String_value>,

"labeltype":<String_value>,

"invoke_labelname":<String_value>,

"flowtype":<Integer_value>,

"description":<String_value>,

"isdefault":<Boolean_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnspolicylabel? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "dnspolicylabel": [ { "__count": "#no"} ] }
```

dnspolicylabel_binding

Binding object which returns the resources bound to dnspolicylabel.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
labelname	<String>	Read-write	Name of the dns policy label.
dnspolicylabel_policybinding_binding	<dnspolicylabel_policybinding_binding[]>	Read-only	policybinding that can be bound to dnspolicylabel.
dnspolicylabel_dnspolicy_binding	<dnspolicylabel_dnspolicy_binding[]>	Read-only	dnspolicy that can be bound to dnspolicylabel.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnspolicylabel_binding/ labelname_value<String>

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "dnspolicylabel_binding": [ {

"labelname":<String_value>,

"dnspolicylabel_policybinding_binding":<dnspolicylabel_policybinding_binding[]_value>,

"dnspolicylabel_dnspolicy_binding":<dnspolicylabel_dnspolicy_binding[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnspolicylabel_binding

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters:

bulkbindings

http:// <netscaler-ip-address> /nitro/v1/config/dnspolicylabel_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "dnspolicylabel_binding": [ {

"labelname":<String_value>,

"dnspolicylabel_policybinding_binding":<dnspolicylabel_policybinding_binding[]_value>,

"dnspolicylabel_dnspolicy_binding":<dnspolicylabel_dnspolicy_binding[]_value>

}]}
```

dnspolicylabel_dnspolicy_binding

Binding object showing the dnspolicy that can be bound to dnspolicylabel.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
labelname	<String>	Read-write	Name of the dns policy label.
labeltype	<String>	Read-write	Type of policy label invocation. Possible values = policylabel
priority	<Integer>	Read-write	Specifies the priority of the policy.
policyname	<String>	Read-write	The dns policy name.
gotopriorityexpression	<String>	Read-write	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
invoke	<Boolean>	Read-write	Invoke flag.
invoke_labelname	<String>	Read-write	Name of the label to invoke if the current policy rule evaluates to TRUE.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/dnspolicylabel_dnspolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"dnspolicylabel_dnspolicy_binding":{
```

```
<b>"labelname":<String_value>,

</b><b>"policyname":<String_value>,

</b><b>"priority":<Integer_value>,

</b>"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>,

"labeltype":<String_value>,

"invoke_labelname":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnspolicylabel_dnspolicy_binding/ labelname_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ dnspolicylabel_dnspolicy_binding/ labelname_value<String> ? **args= policyname:<String_value>, priority: <Integer_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnspolicylabel_dnspolicy_binding/ labelname_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/

dnspolicylabel_dnspolicy_binding/ labelname_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of dnspolicylabel_dnspolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/dnspolicylabel_dnspolicy_binding/ labelname_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the dnspolicylabel_dnspolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "dnspolicylabel_dnspolicy_binding": [ {

"labelname":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"policyname":<String_value>,

"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>,
```

```
"invoke_labelname":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnspolicylabel_dnspolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/dnspolicylabel_dnspolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "dnspolicylabel_dnspolicy_binding": [ {

"labelname":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"policyname":<String_value>,
```

```
"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>,

"invoke_labelname":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnspolicylabel_dnspolicy_binding/ labelname_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"dnspolicylabel_dnspolicy_binding": [ { "__count": "#no"} ] }
```

dnspolicylabel_policybinding_binding

Binding object showing the policybinding that can be bound to dnspolicylabel.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
labelname	<String>	Read-write	Name of the dns policy label.
labeltype	<String>	Read-write	Type of policy label invocation. Possible values = policylabel
priority	<Integer>	Read-write	Specifies the priority of the policy.
policyname	<String>	Read-write	The dns policy name.
gotopriorityexpression	<String>	Read-write	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
invoke	<Boolean>	Read-write	Invoke flag.
invoke_labelname	<String>	Read-write	Name of the label to invoke if the current policy rule evaluates to TRUE.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnspolicylabel_policybinding_binding/ labelname_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ dnspolicylabel_policybinding_binding/ labelname_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of dnspolicylabel_policybinding_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/dnspolicylabel_policybinding_binding/ labelname_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the dnspolicylabel_policybinding_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "dnspolicylabel_policybinding_binding": [ {

"labelname":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"policyname":<String_value>,

"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>,

"invoke_labelname":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnspolicylabel_policybinding_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/dnspolicylabel_policybinding_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "dnspolicylabel_policybinding_binding": [ {

"labelname":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"policyname":<String_value>,

"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>,

"invoke_labelname":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnspolicylabel_policybinding_binding/labelname_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"dnspolicylabel_policybinding_binding": [ { "__count": "#no"} ] }
```

dnsprofile

Configuration for DNS profile resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
dnsprofilename	<String>	Read-write	Name of the DNS profile. Minimum length = 1 Maximum length = 127
recursiveresolution	<String>	Read-write	DNS recursive resolution; if enabled, will do recursive resolution for DNS query when the profile is associated with ADNS service, CS

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Vserver and DNS action. Default value: DISABLED Possible values = ENABLED, DISABLED
dnsquerylogging	<String>	Read-write	DNS query logging; if enabled, DNS query information such as DNS query id, DNS query flags , DNS domain name and DNS query type will be logged. Default value: DISABLED Possible values = ENABLED, DISABLED
dnsanswersecloggin g	<String>	Read-write	DNS answer section; if enabled, answer section in the response will be logged. Default value: DISABLED Possible values = ENABLED, DISABLED
dnsextendedlogging	<String>	Read-write	DNS extended logging; if enabled, authority and additional section in

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			the response will be logged. Default value: DISABLED Possible values = ENABLED, DISABLED
dnserrorlogging	<String>	Read-write	DNS error logging; if enabled, whenever error is encountered in DNS module reason for the error will be logged. Default value: DISABLED Possible values = ENABLED, DISABLED
cacherecords	<String>	Read-write	Cache resource records in the DNS cache. Applies to resource records obtained through proxy configurations only. End resolver and forwarder configurations always cache records in the DNS cache, and you cannot disable this behavior. When you disable record caching, the appliance stops caching server

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			responses. However, cached records are not flushed. The appliance does not serve requests from the cache until record caching is enabled again. Default value: ENABLED Possible values = ENABLED, DISABLED
cachenegativerespo nses	<String>	Read-write	Cache negative responses in the DNS cache. When disabled, the appliance stops caching negative responses except referral records. This applies to all configurations - proxy, end resolver, and forwarder. However, cached responses are not flushed. The appliance does not serve negative responses from the cache until this parameter is enabled again. Default value: ENABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ENABLED, DISABLED
dropmultiqueryrequest	<String>	Read-write	Drop the DNS requests containing multiple queries. When enabled, DNS requests containing multiple queries will be dropped. In case of proxy configuration by default the DNS request containing multiple queries is forwarded to the backend and in case of ADNS and Resolver configuration NOCODE error response will be sent to the client. Default value: DISABLED Possible values = ENABLED, DISABLED
cacheecsresponses	<String>	Read-write	Cache DNS responses with EDNS Client Subnet(ECS) option in the DNS cache. When disabled, the appliance stops caching responses with ECS option.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			This is relevant to proxy configuration. Enabling/disabling support of ECS option when Citrix ADC is authoritative for a GSLB domain is supported using a knob in GSLB vserver. In all other modes, ECS option is ignored. Default value: DISABLED Possible values = ENABLED, DISABLED
insertecs	<String>	Read-write	Insert ECS Option on DNS query. Default value: DISABLED Possible values = ENABLED, DISABLED
replaceecs	<String>	Read-write	Replace ECS Option on DNS query. Default value: DISABLED Possible values = ENABLED, DISABLED
maxcacheableecsprefixlength	<Integer>	Read-write	The maximum ecs prefix length that will be cached.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: 32 Minimum value = 0 Maximum value = 32
maxcacheableecsprefixlength6	<Integer>	Read-write	The maximum ecs prefix length that will be cached for IPv6 subnets. Default value: 128 Minimum value = 0 Maximum value = 128
referencecount	<Integer>	Read-only	Number of entities using this profile.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- UPDATE
- UNSET
- DELETE
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnsprofile **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"dnsprofile":{

<b>"dnsprofilename":<String_value>,

</b>"recursiveresolution":<String_value>,

"dnsquerylogging":<String_value>,
```

```
"dnsanswerseclogging":<String_value>,

"dnsextendedlogging":<String_value>,

"dnserrorlogging":<String_value>,

"cacherecords":<String_value>,

"cachenegativeresponses":<String_value>,

"dropmultiqueryrequest":<String_value>,

"cacheecsresponses":<String_value>,

"insertecs":<String_value>,

"replaceecs":<String_value>,

"maxcacheableecsprefixlength":<Integer_value>,

"maxcacheableecsprefixlength6":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnsprofile **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"dnsprofile":{

<b>"dnsprofilename":<String_value>,

</b>"recursiveresolution":<String_value>,

"dnsquerylogging":<String_value>,

"dnsanswerseclogging":<String_value>,

"dnsextendedlogging":<String_value>,

"dnserrorlogging":<String_value>,

"cacherecords":<String_value>,

"cachenegativeresponses":<String_value>,

"dropmultiqueryrequest":<String_value>,

"cacheecsresponses":<String_value>,

"insertecs":<String_value>,

"replaceecs":<String_value>,

"maxcacheableecsprefixlength":<Integer_value>,

"maxcacheableecsprefixlength6":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnsprofile? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"dnsprofile":{

<b>"dnsprofilename":<String_value>,

</b>"recursiveresolution":true,

"dnsquerylogging":true,

"dnsanswerseclogging":true,

"dnsextendedlogging":true,

"dnserrorlogging":true,

"cacherecords":true,

"cachenegativeresponses":true,

"dropmultiqueryrequest":true,

"cacheecsresponses":true,

"insertecs":true,

"replaceecs":true,

"maxcacheableecsprefixlength":true,

"maxcacheableecsprefixlength6":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnsprofile/ dnsprofilename_value<String>
HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnsprofile **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/dnsprofile? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/dnsprofile? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of dnsprofile resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/dnsprofile? **view=summary**

Use this query-parameter to get the summary output of dnsprofile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/dnsprofile? **pagesize=#no;pageno=#no**

Use this query-parameter to get the dnsprofile resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "dnsprofile": [ {

"dnsprofilename":<String_value>,

"dnsquerylogging":<String_value>,

"recursiveresolution":<String_value>,

"dnsanswerseclogging":<String_value>,

"dnsextendedlogging":<String_value>,

"dnserrorlogging":<String_value>,

"cacherecords":<String_value>,

"cachenegativeresponses":<String_value>,

"dropmultiqueryrequest":<String_value>,

"cacheecsresponses":<String_value>,

"insertecs":<String_value>,

"replaceecs":<String_value>,

"maxcacheableecsprefixlength":<Integer_value>,

"maxcacheableecsprefixlength6":<Integer_value>,

"referencecount":<Integer_value>,

"_nextgenapiresource":<String_value>
```

```
}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnsprofile/ dnsprofilename_value<String>
Query-parameters: attrs http:// <netscaler-ip-address> /nitro/v1/config/dnsprofile/ dnsprofilename_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/dnsprofile/ dnsprofilename_value<String> ? **view=summary**

Use this query-parameter to get the summary output of dnsprofile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "dnsprofile": [ {

"dnsprofilename":<String_value>,

"dnsquerylogging":<String_value>,
```

```
"recursiveresolution":<String_value>,

"dnsanswerseclogging":<String_value>,

"dnsextendedlogging":<String_value>,

"dnserrorlogging":<String_value>,

"cacherecords":<String_value>,

"cachenegativeresponses":<String_value>,

"dropmultiqueryrequest":<String_value>,

"cacheecsresponses":<String_value>,

"insertecs":<String_value>,

"replaceecs":<String_value>,

"maxcacheableecsprefixlength":<Integer_value>,

"maxcacheableecsprefixlength6":<Integer_value>,

"referencecount":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnsprofile? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "dnsprofile": [ { "__count": "#no"} ] }
```

dnsproxyrecords

Configuration for proxy record resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
type	<String>	Read-write	Filter the DNS records to be flushed.e.g flush dns proxyRecords -type A will flush only the A records from the cache. . Possible values = A, NS, CNAME, SOA, MX, AAAA, SRV, RRSIG, NSEC, DNSKEY, PTR, TXT, NAPTR, CAA, SVCB, HTTPS
negrectype	<String>	Read-write	Filter the Negative DNS records i.e NXDOMAIN and NODATA entries to be flushed. e.g flush dns proxyRecords

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			NXDOMAIN will flush only the NXDOMAIN entries from the cache. Possible values = NXDOMAIN, NODATA

Operations

(click to see Properties)

- FLUSH

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

FLUSH

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnsproxyrecords? **action=flush HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"dnsproxyrecords":{

"type":<String_value>,

"negrectype":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

dnsptrrec

Configuration for PTR record resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
reversedomain	<String>	Read-write	Reversed domain name representation of the IPv4 or IPv6 address for which to create the PTR record. Use the "in-addr.arpa." suffix for IPv4 addresses and

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			the "ip6.arpa." suffix for IPv6 addresses. Minimum length = 1
domain	<String>	Read-write	Domain name for which to configure reverse mapping. Minimum length = 1
ttl	<Integer>	Read-write	Time to Live (TTL), in seconds, for the record. TTL is the time for which the record must be cached by DNS proxies. The specified TTL is applied to all the resource records that are of the same record type and belong to the specified domain name. For example, if you add an address record, with a TTL of 36000, to the domain name example.com, the TTLs of all the address records of example.com are changed to 36000. If the TTL is not specified, the Citrix ADC uses either the DNS zone's minimum TTL or, if the SOA record is not available on the appliance, the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			default value of 3600. Default value: 3600 Minimum value = 0 Maximum value = 2147483647
ecssubnet	<String>	Read-write	Subnet for which the cached PTR record need to be removed.
type	<String>	Read-write	Type of records to display. Available settings function as follows: * ADNS - Display all authoritative address records. * PROXY - Display all proxy address records. * ALL - Display all address records. Possible values = ALL, ADNS, PROXY
nodeid	<Integer>	Read-write	Unique number that identifies the cluster node. Minimum value = 0 Maximum value = 31

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
authtype	<String>	Read-only	Authentication type. Possible values = ALL, ADNS, PROXY
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnsptrrec **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"dnsptrrec":{

<b>"reversedomain":<String_value>,

</b><b>"domain":<String_value>,

</b>"ttl":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnsptrrec/ reversedomain_value<String>
Query-parameters: args=ecssubnet: <String_value> ,domain: <String_value>
get (all)
URL: http:// <netscaler-ip-address> /nitro/v1/config/dnsptrrec **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/dnsptrrec? **args=reversedomain: <String_value> ,type: <String_value> ,nodeid: <Integer_value>**

Use this query-parameter to get dnsptrrec resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/config/dnsptrrec? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/dnsptrrec? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of dnsptrrec resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/dnsptrrec? **view=summary**

Use this query-parameter to get the summary output of dnsptrrec resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/dnsptrrec? **pagesize=#no;pageno=#no**

Use this query-parameter to get the dnsptrrec resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "dnsptrrec": [ {

reversedomain:<String_value>,type:<String_value>,nodeid:<Integer_value>"do
main":<String_value>,

"ttl":<Integer_value>,

"authtype":<String_value>,

"ecssubnet":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

get
URL: http:// <netscaler-ip-address> /nitro/v1/config/dnsptrrec/ reversedomain_value<String>
Query-parameters: attrs http:// <netscaler-ip-address> /nitro/v1/config/dnsptrrec/ reversedomain_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/dnsptrrec/ reversedomain_value<String> ? **view=summary**

Use this query-parameter to get the summary output of dnsptrrec resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "dnsptrrec": [ {

reversedomain:<String_value>,type:<String_value>,nodeid:<Integer_value>"do
main":<String_value>,

"ttl":<Integer_value>,

"authtype":<String_value>,

"ecssubnet":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

count
URL: http:// <netscaler-ip-address> /nitro/v1/config/dnsptrrec? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "dnsptrrec": [ { "__count": "#no"} ] }
```

dnssoarec

Configuration for SOA record resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
domain	<String>	Read-write	Domain name for which to add the SOA record. Minimum length = 1
originserver	<String>	Read-write	Domain name of the name server that responds authoritatively for the domain. Minimum length = 1
contact	<String>	Read-write	Email address of the contact to whom domain issues can be addressed. In the email address, replace the @ sign with a period (.). For example, enter domainadmin.example.com instead of domainadmin@example.com. Minimum length = 1
serial	<Integer>	Read-write	The secondary server uses this parameter to determine whether it

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			requires a zone transfer from the primary server. Default value: 100 Minimum value = 0 Maximum value = 4294967294
refresh	<Integer>	Read-write	Time, in seconds, for which a secondary server must wait between successive checks on the value of the serial number. Default value: 3600 Minimum value = 0 Maximum value = 4294967294
retry	<Integer>	Read-write	Time, in seconds, between retries if a secondary server's attempt to contact the primary server for a zone refresh fails. Default value: 3 Minimum value = 0 Maximum value = 4294967294
expire	<Integer>	Read-write	Time, in seconds, after which the zone data on a secondary name server can no longer be considered

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			authoritative because all refresh and retry attempts made during the period have failed. After the expiry period, the secondary server stops serving the zone. Typically one week. Not used by the primary server. Default value: 3600 Minimum value = 0 Maximum value = 4294967294
minimum	<Integer>	Read-write	Default time to live (TTL) for all records in the zone. Can be overridden for individual records. Default value: 5 Minimum value = 0 Maximum value = 2147483647
ttl	<Integer>	Read-write	Time to Live (TTL), in seconds, for the record. TTL is the time for which the record must be cached by DNS proxies. The specified TTL is applied to all the resource records that

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			are of the same record type and belong to the specified domain name. For example, if you add an address record, with a TTL of 36000, to the domain name example.com, the TTLs of all the address records of example.com are changed to 36000. If the TTL is not specified, the Citrix ADC uses either the DNS zone's minimum TTL or, if the SOA record is not available on the appliance, the default value of 3600. Default value: 3600 Minimum value = 0 Maximum value = 2147483647
ecssubnet	<String>	Read-write	Subnet for which the cached SOA record need to be removed.
type	<String>	Read-write	Type of records to display. Available settings function as follows:

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			* ADNS - Display all authoritative address records. * PROXY - Display all proxy address records. * ALL - Display all address records. Possible values = ALL, ADNS, PROXY
nodeid	<Integer>	Read-write	Unique number that identifies the cluster node. Minimum value = 0 Maximum value = 31
authtype	<String>	Read-only	Record type. Possible values = ALL, ADNS, PROXY
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE

- UNSET
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnssoarec **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"dnssoarec":{

<b>"domain":<String_value>,

</b><b>"originserver":<String_value>,

</b><b>"contact":<String_value>,

</b>"serial":<Integer_value>,

"refresh":<Integer_value>,

"retry":<Integer_value>,

"expire":<Integer_value>,

"minimum":<Integer_value>,

"ttl":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnssoarec/ domain_value<String> **Query-parameters: args=ecssubnet: <String_value>**
update
URL: http:// <netscaler-ip-address> /nitro/v1/config/dnssoarec **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"dnssoarec":{

<b>"domain":<String_value>,

</b>"originserver":<String_value>,

"contact":<String_value>,

"serial":<Integer_value>,

"refresh":<Integer_value>,

"retry":<Integer_value>,

"expire":<Integer_value>,

"minimum":<Integer_value>,

"ttl":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

unset

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnssoarec? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"dnssoarec":{

<b>"domain":<String_value>,
```

```
</b>"serial":true,

"refresh":true,

"retry":true,

"expire":true,

"minimum":true,

"ttl":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error
get (all)
URL: http:// <netscaler-ip-address> /nitro/v1/config/dnssoarec **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/dnssoarec? **args=domain: <String_value> ,type: <String_value> ,nodeid: <Integer_value>**

Use this query-parameter to get dnssoarec resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/config/dnssoarec? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/dnssoarec? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of dnssoarec resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/dnssoarec? **view=summary**

Use this query-parameter to get the summary output of dnssoarec resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/dnssoarec? **pagesize=#no;pageno=#no**

Use this query-parameter to get the dnssoarec resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "dnssoarec": [ {

domain:<String_value>,type:<String_value>,nodeid:<Integer_value>"originser
ver":<String_value>,

"contact":<String_value>,

"serial":<Integer_value>,

"refresh":<Integer_value>,

"retry":<Integer_value>,

"expire":<Integer_value>,

"minimum":<Integer_value>,

"ttl":<Integer_value>,

"authtype":<String_value>,
```

```
"ecssubnet":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

get
URL: http:// <netscaler-ip-address> /nitro/v1/config/dnssoarec/ domain_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/dnssoarec/ domain_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/dnssoarec/ domain_value<String> ? **view=summary**

Use this query-parameter to get the summary output of dnssoarec resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "dnssoarec": [ {

domain:<String_value>,type:<String_value>,nodeid:<Integer_value>"originser
ver":<String_value>,

"contact":<String_value>,

"serial":<Integer_value>,

"refresh":<Integer_value>,

"retry":<Integer_value>,

"expire":<Integer_value>,

"minimum":<Integer_value>,

"ttl":<Integer_value>,

"authtype":<String_value>,

"ecssubnet":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

count

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnssoarec? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "dnssoarec": [ { "__count": "#no"} ] }
```

dnssrvrec

Configuration for server record resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
domain	<String>	Read-write	Domain name, which, by convention, is prefixed by the symbolic name of the desired service and the symbolic name of the desired protocol, each with an underscore (_) prepended. For example, if an SRV-aware client wants to discover a SIP service that is provided over UDP, in the domain example.com, the client performs a lookup for _sip._udp.example.com. Minimum length = 1
target	<String>	Read-write	Target host for the specified service.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
priority	<Integer>	Read-write	Integer specifying the priority of the target host. The lower the number, the higher the priority. If multiple target hosts have the same priority, selection is based on the Weight parameter. Minimum value = 0 Maximum value = 65535
weight	<Integer>	Read-write	Weight for the target host. Aids host selection when two or more hosts have the same priority. A larger number indicates greater weight. Minimum value = 0 Maximum value = 65535
port	<Integer>	Read-write	Port on which the target host listens for client requests. Minimum value = 0 Maximum value = 65535
ttl	<Integer>	Read-write	Time to Live (TTL), in seconds, for the record. TTL is the time for which the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			record must be cached by DNS proxies. The specified TTL is applied to all the resource records that are of the same record type and belong to the specified domain name. For example, if you add an address record, with a TTL of 36000, to the domain name example.com, the TTLs of all the address records of example.com are changed to 36000. If the TTL is not specified, the Citrix ADC uses either the DNS zone's minimum TTL or, if the SOA record is not available on the appliance, the default value of 3600. Default value: 3600 Minimum value = 0 Maximum value = 2147483647
ecssubnet	<String>	Read-write	Subnet for which the cached SRV record need to be removed.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
type	<String>	Read-write	Type of records to display. Available settings function as follows: * ADNS - Display all authoritative address records. * PROXY - Display all proxy address records. * ALL - Display all address records. Possible values = ALL, ADNS, PROXY
nodeid	<Integer>	Read-write	Unique number that identifies the cluster node. Minimum value = 0 Maximum value = 31
authtype	<String>	Read-only	Record type. Possible values = ALL, ADNS, PROXY
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnssrvrec **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"dnssrvrec":{

<b>"domain":<String_value>,

</b><b>"target":<String_value>,

</b><b>"priority":<Integer_value>,

</b><b>"weight":<Integer_value>,

</b><b>"port":<Integer_value>,

</b>"ttl":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnssrvrec/ domain_value<String> **Query-parameters: args= target:<String_value>, ecssubnet: <String_value>**
update
URL: http:// <netscaler-ip-address> /nitro/v1/config/dnssrvrec **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"dnssrvrec":{

<b>"domain":<String_value>,

</b><b>"target":<String_value>,

</b>"priority":<Integer_value>,

"weight":<Integer_value>,

"port":<Integer_value>,

"ttl":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

unset

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnssrvrec? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"dnssrvrec":{

<b>"domain":<String_value>,

</b><b>"target":<String_value>,

</b>"ttl":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error
get (all)
URL: http:// <netscaler-ip-address> /nitro/v1/config/dnssrvrec **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/dnssrvrec? **args=domain: <String_value> ,target: <String_value> ,type: <String_value> ,nodeid: <Integer_value>**

Use this query-parameter to get dnssrvrec resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/config/dnssrvrec? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/dnssrvrec? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of dnssrvrec resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/dnssrvrec? **view=summary**

Use this query-parameter to get the summary output of dnssrvrec resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/dnssrvrec? **pagesize=#no;pageno=#no**

Use this query-parameter to get the dnssrvrec resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "dnssrvrec": [ {

domain:<String_value>,target:<String_value>,type:<String_value>,nodeid:<In
teger_value>"priority":<Integer_value>,

"weight":<Integer_value>,

"port":<Integer_value>,

"ttl":<Integer_value>,

"authtype":<String_value>,

"ecssubnet":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

count
URL: http:// <netscaler-ip-address> /nitro/v1/config/dnssrvrec? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "dnssrvrec": [ { "__count": "#no"} ] }
```

dnssubnetcache

Configuration for subnet cache resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ecssubnet	<String>	Read-write	ECS Subnet.
all	<Boolean>	Read-write	Flush all the ECS subnets from the DNS cache.
nodeid	<Integer>	Read-write	Unique number that identifies the cluster node. Minimum value = 0 Maximum value = 31
hostname	<String>	Read-only	Domain name. Minimum length = 1
nextrecs	<String[]>	Read-only	An array of record types associated with the domain name. Possible values = A, NS, CNAME, SOA, MX, AAAA, SRV, RRSIG, NSEC, DNSKEY, PTR,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			TXT, NAPTR, CAA, SVCB, HTTPS
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- FLUSH
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

FLUSH

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnssubnetcache? **action=flush HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"dnssubnetcache":{

"ecssubnet":<String_value>,

"all":<Boolean_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnssubnetcache **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/dnssubnetcache? **args=ecssubnet: <String_value> ,nodeid: <Integer_value>**

Use this query-parameter to get dnssubnetcache resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/config/dnssubnetcache? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/dnssubnetcache? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of dnssubnetcache resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/dnssubnetcache? **view=summary**

Use this query-parameter to get the summary output of dnssubnetcache resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/dnssubnetcache? **pagesize=#no;pageno=#no**

Use this query-parameter to get the dnssubnetcache resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "dnssubnetcache": [ {

ecssubnet:<String_value>,nodeid:<Integer_value>"hostname":<String_value>,

"nextrecs":<String[]_value>,

"_nextgenapiresource":<String_value>
```

```
}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnssubnetcache/ ecssubnet_value<String>
Query-parameters: attrs http:// <netscaler-ip-address> /nitro/v1/config/dnssubnetcache/ ecssubnet_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/dnssubnetcache/ ecssubnet_value<String> ? **view=summary**

Use this query-parameter to get the summary output of dnssubnetcache resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "dnssubnetcache": [ {

ecssubnet:<String_value>,nodeid:<Integer_value>"hostname":<String_value>,

"nextrecs":<String[]_value>,
```

```
"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnssubnetcache? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "dnssubnetcache": [ { "__count": "#no"} ] }
```

dnssuffix

Configuration for DNS suffix resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
Dnssuffix	<String>	Read-write	Suffix to be appended when resolving domain

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			names that are not fully qualified. Minimum length = 1
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnssuffix **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"dnssuffix":{

<b>"Dnssuffix":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnssuffix/ Dnssuffix_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnssuffix **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/dnssuffix? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/dnssuffix? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of dnssuffix resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/dnssuffix? **view=summary**

Use this query-parameter to get the summary output of dnssuffix resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/dnssuffix? **pagesize=#no;pageno=#no**

Use this query-parameter to get the dnssuffix resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "dnssuffix": [ {

"Dnssuffix":<String_value>,
```

```
"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnssuffix/ Dnssuffix_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/dnssuffix/ Dnssuffix_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/dnssuffix/ Dnssuffix_value<String> ? **view=summary**

Use this query-parameter to get the summary output of dnssuffix resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "dnssuffix": [ {

"Dnssuffix":<String_value>,
```

```
"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnssuffix? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "dnssuffix": [ { "__count": "#no"} ] }
```

dnssvcbrec

Configuration for SVCB/HTTPS service binding record resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
domain	<String>	Read-write	Domain name for the SVCB/HTTPS record. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
priority	<Integer>	Read-write	Service priority (0 for AliasMode, >0 for ServiceMode). Minimum value = 0 Maximum value = 65535
targetname	<String>	Read-write	Target domain name. Minimum length = 1
svcbtype	<String>	Read-write	Service type: SVCB or HTTPS. Default value: SVCB Possible values = SVCB, HTTPS
alpn	<String>	Read-write	Comma-separated list of ALPN protocol identifiers. Minimum length = 1
port	<Integer>	Read-write	Port number for the service. Minimum value = 1 Maximum value = 65535
ipv4hint	<String>	Read-write	Comma-separated list of IPv4 hint addresses. Minimum length = 1
ipv6hint	<String>	Read-write	Comma-separated list of IPv6 hint addresses. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
encryptedclienthello	<String>	Read-write	Base64-encoded ECH configuration. Minimum length = 1
nodefaultalpn	<Boolean>	Read-write	Indicates no default ALPN protocols. Default value: 0
mandatory	<String>	Read-write	Comma-separated list of mandatory SvcParam keys. Minimum length = 1
ttl	<Integer>	Read-write	Time to Live (TTL) in seconds. Default value: 3600 Minimum value = 0 Maximum value = 2147483647
type	<String>	Read-write	Type of records: ADNS, PROXY, or ALL. Possible values = ALL, ADNS, PROXY
nodeid	<Integer>	Read-write	Unique number that identifies the cluster node. Minimum value = 0 Maximum value = 31
ecssubnet	<String>	Read-only	Subnet for which this particular record is cached. Subnet

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			caching will occur for responses with EDNS Client Subnet (ECS) option. Applies to resource records obtained through proxy configurations only.
authtype	<String>	Read-only	Record type (ADNS/PROXY/ALL). Possible values = ALL, ADNS, PROXY
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnssvcbrec **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"dnssvcbrec":{

<b>"domain":<String_value>,

</b><b>"priority":<Integer_value>,

</b><b>"targetname":<String_value>,

</b>"svcbtype":<String_value>,

"alpn":<String_value>,

"port":<Integer_value>,

"ipv4hint":<String_value>,
```

```
"ipv6hint":<String_value>,

"encryptedclienthello":<String_value>,

"nodefaultalpn":<Boolean_value>,

"mandatory":<String_value>,

"ttl":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnssvcbrec/ domain_value<String> **Query-parameters: args=targetname: <String_value> ,priority: <Integer_value> ,svcbtype: <String_value>**
update
URL: http:// <netscaler-ip-address> /nitro/v1/config/dnssvcbrec **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"dnssvcbrec":{

<b>"domain":<String_value>,

</b><b>"priority":<Integer_value>,

</b><b>"targetname":<String_value>,

</b>"svcbtype":<String_value>,
```

```
"alpn":<String_value>,

"port":<Integer_value>,

"ipv4hint":<String_value>,

"ipv6hint":<String_value>,

"encryptedclienthello":<String_value>,

"nodefaultalpn":<Boolean_value>,

"mandatory":<String_value>,

"ttl":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

unset

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnssvcbrec? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"dnssvcbrec":{

<b>"domain":<String_value>,

</b><b>"priority":<Integer_value>,

</b><b>"targetname":<String_value>,
```

```
</b>"svcbtype":<String_value>,

"alpn":true,

"port":true,

"ipv4hint":true,

"ipv6hint":true,

"encryptedclienthello":true,

"nodefaultalpn":true,

"mandatory":true,

"ttl":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error
get (all)
URL: http:// <netscaler-ip-address> /nitro/v1/config/dnssvcbrec **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/dnssvcbrec? **args=domain: <String_value> ,svcbtype: <String_value> ,type: <String_value> ,nodeid: <Integer_value>**

Use this query-parameter to get dnssvcbrec resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/config/dnssvcbrec? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/dnssvcbrec? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of dnssvcbrec resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/dnssvcbrec? **view=summary**

Use this query-parameter to get the summary output of dnssvcbrec resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/dnssvcbrec? **pagesize=#no;pageno=#no**

Use this query-parameter to get the dnssvcbrec resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "dnssvcbrec": [ {

domain:<String_value>,svcbtype:<String_value>,type:<String_value>,nodeid:<
Integer_value>"priority":<Integer_value>,

"targetname":<String_value>,

"ttl":<Integer_value>,

"ecssubnet":<String_value>,

"alpn":<String_value>,

"nodefaultalpn":<Boolean_value>,
```

```
"ipv4hint":<String_value>,

"ipv6hint":<String_value>,

"encryptedclienthello":<String_value>,

"mandatory":<String_value>,

"port":<Integer_value>,

"authtype":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

count

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnssvcbrec? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "dnssvcbrec": [ { "__count": "#no"} ] }
```

dnstxtrec

Configuration for TXT record resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
domain	<String>	Read-write	Name of the domain for the TXT record. Minimum length = 1
String	<String[]>	Read-write	Information to store in the TXT resource record. Enclose the string in single or double quotation marks. A TXT resource record can contain up to six strings, each of which can contain up to 255 characters. If you want to add a string of more than 255 characters, evaluate whether splitting it into two or more smaller strings, subject to the six-string limit, works for you. Maximum length = 255
ttl	<Integer>	Read-write	Time to Live (TTL), in seconds, for the record. TTL is the time for which the record must be cached by DNS proxies. The specified TTL is applied to all the resource records that

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			are of the same record type and belong to the specified domain name. For example, if you add an address record, with a TTL of 36000, to the domain name example.com, the TTLs of all the address records of example.com are changed to 36000. If the TTL is not specified, the Citrix ADC uses either the DNS zone's minimum TTL or, if the SOA record is not available on the appliance, the default value of 3600. Default value: 3600 Minimum value = 0 Maximum value = 2147483647
recordid	<Integer>	Read-write	Unique, internally generated record ID. View the details of the TXT record to obtain its record ID. Mutually exclusive with the string parameter. Minimum value = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum value = 65535
ecssubnet	<String>	Read-write	Subnet for which the cached TXT record need to be removed.
type	<String>	Read-write	Type of records to display. Available settings function as follows: * ADNS - Display all authoritative address records. * PROXY - Display all proxy address records. * ALL - Display all address records. Default value: ADNS Possible values = ALL, ADNS, PROXY
nodeid	<Integer>	Read-write	Unique number that identifies the cluster node. Minimum value = 0 Maximum value = 31
authtype	<String>	Read-only	Authentication type.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ALL, ADNS, PROXY
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnstxtrec **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"dnstxtrec":{

<b>"domain":<String_value>,

</b><b>"String":<String[]_value>,

</b>"ttl":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnstxtrec/ domain_value<String> **Query-parameters: args=String: <String_value> ,recordid: <Integer_value> ,ecssubnet: <String_value>**
get (all)
URL: http:// <netscaler-ip-address> /nitro/v1/config/dnstxtrec **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/dnstxtrec? **args=domain: <String_value> ,type: <String_value> ,nodeid: <Integer_value>**

Use this query-parameter to get dnstxtrec resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/config/dnstxtrec? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/dnstxtrec? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of dnstxtrec resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/dnstxtrec? **view=summary**

Use this query-parameter to get the summary output of dnstxtrec resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/dnstxtrec? **pagesize=#no;pageno=#no**

Use this query-parameter to get the dnstxtrec resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "dnstxtrec": [ {

domain:<String_value>,type:<String_value>,nodeid:<Integer_value>"String":<
String[]_value>,
```

```
"ecssubnet":<String_value>,

"ttl":<Integer_value>,

"recordid":<Integer_value>,

"authtype":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

get
URL: http:// <netscaler-ip-address> /nitro/v1/config/dnstxtrec/ domain_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/dnstxtrec/ domain_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/dnstxtrec/ domain_value<String> ? **view=summary**

Use this query-parameter to get the summary output of dnstxtrec resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "dnstxtrec": [ {

domain:<String_value>,type:<String_value>,nodeid:<Integer_value>"String":<
String[]_value>,

"ecssubnet":<String_value>,

"ttl":<Integer_value>,

"recordid":<Integer_value>,

"authtype":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

count

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnstxtrec? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "dnstxtrec": [ { "__count": "#no"} ] }
```

dnsview

Configuration for DNS view resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
viewname	<String>	Read-write	Name for the DNS view. Minimum length = 1
flags	<Integer>	Read-only	Flags controlling display.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnsview **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"dnsview":{

<b>"viewname":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnsview/ viewname_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnsview **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/dnsview? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/dnsview? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of dnsview resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/dnsview? **view=summary**

Use this query-parameter to get the summary output of dnsview resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/dnsview? **pagesize=#no;pageno=#no**

Use this query-parameter to get the dnsview resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "dnsview": [ {

"viewname":<String_value>,

"servicename":<String_value>,

"flags":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnsview/ viewname_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/dnsview/ viewname_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/dnsview/ viewname_value<String> ? **view=summary**

Use this query-parameter to get the summary output of dnsview resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "dnsview": [ {

"viewname":<String_value>,

"servicename":<String_value>,

"flags":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnsview? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "dnsview": [ { "__count": "#no"} ] }
```

dnsview_binding

Binding object which returns the resources bound to dnsview.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
viewname	<String>	Read-write	Name of the view to display. Minimum length = 1
dnsview_gslbservice_binding	<dnsview_gslbservice_binding[]>	Read-only	gslbservice that can be bound to dnsview.
dnsview_dnspolicy_binding	<dnsview_dnspolicy_binding[]>	Read-only	dnspolicy that can be bound to dnsview.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnsview_binding/ viewname_value<String>
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "dnsview_binding": [ {

"viewname":<String_value>,

"dnsview_dnspolicy_binding":<dnsview_dnspolicy_binding[]_value>,
```

```
"dnsview_gslbservice_binding":<dnsview_gslbservice_binding[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnsview_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/dnsview_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "dnsview_binding": [ {

"viewname":<String_value>,

"dnsview_dnspolicy_binding":<dnsview_dnspolicy_binding[]_value>,

"dnsview_gslbservice_binding":<dnsview_gslbservice_binding[]_value>

}]}
```

dnsview_dnspolicy_binding

Binding object showing the dnspolicy that can be bound to dnsview.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
viewname	<String>	Read-write	Name of the view to display. Minimum length = 1
dnspolicyname	<String>	Read-write	dnspolicy name of this view.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.
- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnsview_dnspolicy_binding/ viewname_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ dnsview_dnspolicy_binding/ viewname_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of dnsview_dnspolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/dnsview_dnspolicy_binding/ viewname_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the dnsview_dnspolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "dnsview_dnspolicy_binding": [ {

"viewname":<String_value>,

"dnspolicyname":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnsview_dnspolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/dnsview_dnspolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "dnsview_dnspolicy_binding": [ {

"viewname":<String_value>,

"dnspolicyname":<String_value>
```

```
}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnsview_dnspolicy_binding/viewname_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"dnsview_dnspolicy_binding": [ { "__count": "#no"} ] }
```

dnsview_gslbservice_binding

Binding object showing the gslbservice that can be bound to dnsview.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
gslbservicename	<String>	Read-write	Service name of the service using this view.
viewname	<String>	Read-write	Name of the view to display.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum length = 1
ipaddress	<String>	Read-only	IP of the service corresponding to the given view.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnsview_gslbservice_binding/ viewname_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ dnsview_gslbservice_binding/ viewname_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of dnsview_gslbservice_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/dnsview_gslbservice_binding/ viewname_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the dnsview_gslbservice_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "dnsview_gslbservice_binding": [ {

"gslbservicename":<String_value>,

"viewname":<String_value>,

"ipaddress":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnsview_gslbservice_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/dnsview_gslbservice_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "dnsview_gslbservice_binding": [ {

"gslbservicename":<String_value>,

"viewname":<String_value>,

"ipaddress":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnsview_gslbservice_binding/ viewname_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"dnsview_gslbservice_binding": [ { "__count": "#no"} ] }
```

dnszone

Configuration for DNS zone resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
zonename	<String>	Read-write	Name of the zone to create. Minimum length = 1
proxymode	<String>	Read-write	Deploy the zone in proxy mode. Enable in the following scenarios:

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			* The load balanced DNS servers are authoritative for the zone and all resource records that are part of the zone. * The load balanced DNS servers are authoritative for the zone, but the Citrix ADC owns a subset of the resource records that belong to the zone (partial zone ownership configuration). Typically seen in global server load balancing (GSLB) configurations, in which the appliance responds authoritatively to queries for GSLB domain names but forwards queries for other domain names in the zone to the load balanced servers. In either scenario, do not create the zone's Start of Authority (SOA) and

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			name server (NS) resource records on the appliance. Disable if the appliance is authoritative for the zone, but make sure that you have created the SOA and NS records on the appliance before you create the zone. Default value: YES Possible values = YES, NO
dnssecoffload	<String>	Read-write	Enable dnssec offload for this zone. Default value: DISABLED Possible values = ENABLED, DISABLED
nsec	<String>	Read-write	Enable nsec generation for dnssec offload. Default value: DISABLED Possible values = ENABLED, DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
keyname	<String[]>	Read-write	Name of the public/ private DNS key pair with which to sign the zone. You can sign a zone with up to four keys. Minimum length = 1
type	<String>	Read-write	Type of zone to display. Mutually exclusive with the DNS Zone (zoneName) parameter. Available settings function as follows: * ADNS - Display all the zones for which the Citrix ADC is authoritative. * PROXY - Display all the zones for which the Citrix ADC is functioning as a proxy server. * ALL - Display all the zones configured on the appliance. Possible values = ALL, ADNS, PROXY
flags	<Integer>	Read-only	Flags controlling display.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- UPDATE
- UNSET
- DELETE
- SIGN
- UNSIGN
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnszone **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"dnszone":{

<b>"zonename":<String_value>,

</b><b>"proxymode":<String_value>,

</b>"dnssecoffload":<String_value>,

"nsec":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnszone **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"dnszone":{

<b>"zonename":<String_value>,

</b>"proxymode":<String_value>,

"dnssecoffload":<String_value>,

"nsec":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnszone? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"dnszone":{

<b>"zonename":<String_value>,

</b>"proxymode":true,

"dnssecoffload":true,

"nsec":true
```

```
}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnszone/ zonename_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

SIGN

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnszone? **action=sign HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"dnszone":{

<b>"zonename":<String_value>,

</b>"keyname":<String[]_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSIGN

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnszone? **action=unsign HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"dnszone":{

<b>"zonename":<String_value>,

</b>"keyname":<String[]_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnszone **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/dnszone? **args=zonename: <String_value> ,type: <String_value>**

Use this query-parameter to get dnszone resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/config/dnszone? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/dnszone? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of dnszone resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/dnszone? **view=summary**

Use this query-parameter to get the summary output of dnszone resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/dnszone? **pagesize=#no;pageno=#no**

Use this query-parameter to get the dnszone resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "dnszone": [ {

zonename:<String_value>,type:<String_value>"proxymode":<String_value>,

"flags":<Integer_value>,

"nsecbitarray":<String[]_value>,

"dnssecoffload":<String_value>,

"nsec":<String_value>,
```

```
"keyname":<String[]_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnszone/ zonename_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/dnszone/ zonename_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/dnszone/ zonename_value<String> ? **view=summary**

Use this query-parameter to get the summary output of dnszone resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "dnszone": [ {

zonename:<String_value>,type:<String_value>"proxymode":<String_value>,

"flags":<Integer_value>,

"nsecbitarray":<String[]_value>,

"dnssecoffload":<String_value>,

"nsec":<String_value>,

"keyname":<String[]_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnszone? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "dnszone": [ { "__count": "#no"} ] }
```

dnszone_binding

Binding object which returns the resources bound to dnszone.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
zonename	<String>	Read-write	Name of the zone. Mutually exclusive with the type parameter. Minimum length = 1
dnszone_domain_binding	<dnszone_domain_binding[]>	Read-only	domain that can be bound to dnszone.
dnszone_dnskey_binding	<dnszone_dnskey_binding[]>	Read-only	dnskey that can be bound to dnszone.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnszone_binding/ zonename_value<String>
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "dnszone_binding": [ {

"zonename":<String_value>,

"dnszone_dnskey_binding":<dnszone_dnskey_binding[]_value>,

"dnszone_domain_binding":<dnszone_domain_binding[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnszone_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/dnszone_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "dnszone_binding": [ {

"zonename":<String_value>,

"dnszone_dnskey_binding":<dnszone_dnskey_binding[]_value>,

"dnszone_domain_binding":<dnszone_domain_binding[]_value>

}]}
```

dnszone_dnskey_binding

Binding object showing the dnskey that can be bound to dnszone.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
keyname	<String[]>	Read-write	Name of the public/ private DNS key pair with which to sign the zone. You can sign a zone with up to four keys. Minimum length = 1
zonename	<String>	Read-write	Name of the zone. Mutually exclusive with the type parameter. Minimum length = 1
expires	<Integer>	Read-only	Time period for which to consider the key valid, after the key is used to sign a zone.
siginceptiontime	<Integer[]>	Read-only	The time when sign was done with this key. Minimum value = 1
signed	<Integer>	Read-only	Integer which denote status of keys.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnszone_dnskey_binding/ zonename_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ dnszone_dnskey_binding/ zonename_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of dnszone_dnskey_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/dnszone_dnskey_binding/ zonename_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the dnszone_dnskey_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "dnszone_dnskey_binding": [ {

"keyname":<String[]_value>,

"zonename":<String_value>,

"expires":<Integer_value>,

"siginceptiontime":<Integer[]_value>,

"signed":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnszone_dnskey_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/dnszone_dnskey_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "dnszone_dnskey_binding": [ {

"keyname":<String[]_value>,

"zonename":<String_value>,

"expires":<Integer_value>,

"siginceptiontime":<Integer[]_value>,

"signed":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnszone_dnskey_binding/ zonename_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"dnszone_dnskey_binding": [ { "__count": "#no"} ] }
```

dnszone_domain_binding

Binding object showing the domain that can be bound to dnszone.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
zonename	<String>	Read-write	Name of the zone. Mutually exclusive with the type parameter. Minimum length = 1
domain	<String>	Read-write	Domain name that belongs to the given zone.
nextrecs	<String[]>	Read-only	An array of record types associated with the nsec record. Possible values = A, NS, CNAME, SOA, MX, AAAA, SRV, RRSIG, NSEC, DNSKEY, PTR, TXT, NAPTR, CAA, SVCB, HTTPS
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnszone_domain_binding/ zonename_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ dnszone_domain_binding/ zonename_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of dnszone_domain_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/dnszone_domain_binding/ zonename_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the dnszone_domain_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "dnszone_domain_binding": [ {

"zonename":<String_value>,

"domain":<String_value>,

"nextrecs":<String[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnszone_domain_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/dnszone_domain_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "dnszone_domain_binding": [ {

"zonename":<String_value>,

"domain":<String_value>,

"nextrecs":<String[]_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/dnszone_domain_binding/zonename_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"dnszone_domain_binding": [ { "__count": "#no"} ] }
```

dps

Dps

Citrix ADC DPS configuration.

NAME	DESCRIPTION
dpsparameter	Configuration for dps parameter

dpsparameter

Configuration for dps parameter resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
customerid	<String>	Read-write	Customer ID of the Citrix Cloud customer. Default value: "None" Minimum length = 1
deployment	<String>	Read-write	Describes if the customer is connecting to Commerical/ JapanCloud/Gov

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Citrix Cloud customer. Default value: COMMERCIAL Possible values = COMMERCIAL, GOV, JAPANCLOUD
serviceurl	<String>	Read-write	Service URL of the Citrix Cloud customer. Minimum length = 1
builtin	<String[]>	Read-only	Indicates that a variable is a built-in (SYSTEM INTERNAL) type. Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL
feature	<String>	Read-only	The feature to be checked while applying this config.
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- UPDATE
- UNSET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/dpsparameter **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"dpsparameter":{

"customerid":<String_value>,

"deployment":<String_value>,

"serviceurl":<String_value>
```

```
}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/dpsparameter? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"dpsparameter":{

"customerid":true,

"deployment":true,

"serviceurl":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/dpsparameter **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "dpsparameter": [ {

"customerid":<String_value>,

"deployment":<String_value>,

"serviceurl":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

endpoint

Endpoint

Lables attached to various endpoints

NAME	DESCRIPTION
endpointinfo	Configuration for Information

endpointinfo

Configuration for Information resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
endpointkind	<String>	Read-write	Endpoint kind. Currently, IP endpoints are supported. Default value: IP Possible values = IP
endpointname	<String>	Read-write	Name of endpoint, depends on kind. For IP Endpoint - IP address. Minimum length = 1
endpointmetadata	<String>	Read-write	String of qualifiers, in dotted notation, structured metadata for an endpoint. Each qualifier is more specific than the one that precedes it, as in cluster.namespace.service. For example: cluster.default.frontend. Note: A qualifier that includes a dot (.) or space ( ) must be enclosed in double quotation marks. Minimum length = 1
endpointlabelsjson	<String>	Read-write	String representing labels in json form.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum length 16K. Minimum length = 1
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- UPDATE
- UNSET
- DELETE
- GET (ALL)
- COUNT
- CLEAR

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/endpointinfo **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"endpointinfo":{

"endpointkind":<String_value>,

<b>"endpointname":<String_value>,

</b>"endpointmetadata":<String_value>,

"endpointlabelsjson":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/endpointinfo **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"endpointinfo":{

"endpointkind":<String_value>,

<b>"endpointname":<String_value>,

</b>"endpointmetadata":<String_value>,

"endpointlabelsjson":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/endpointinfo? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"endpointinfo":{

"endpointkind":<String_value>,

<b>"endpointname":<String_value>,

</b>"endpointmetadata":true,

"endpointlabelsjson":true
```

```
}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/endpointinfo/ endpointkind_value<String>
Query-parameters: args= endpointname:<String_value>

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

CLEAR

URL: http:// <netscaler-ip-address> /nitro/v1/config/endpointinfo? **action=clear HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"endpointinfo":{

"endpointkind":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/endpointinfo **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/endpointinfo? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/endpointinfo? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of endpointinfo resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/endpointinfo? **view=summary**

Use this query-parameter to get the summary output of endpointinfo resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/endpointinfo? **pagesize=#no;pageno=#no**

Use this query-parameter to get the endpointinfo resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "endpointinfo": [ {

"endpointkind":<String_value>,

"endpointname":<String_value>,

"endpointmetadata":<String_value>,

"endpointlabelsjson":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/endpointinfo? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "endpointinfo": [ { "__count": "#no"} ] }
```

feo

Front-end-optimization

Front end optimization configuration. The system's feature to optimize Web content for performance.

NAME	DESCRIPTION
feoaction	Configuration for Front end optimization action
feoglobal_binding	Binding object showing the resources that can be bound to feoglobal
feoglobal_feopolicy_binding	Binding object showing the feopolicy that can be bound to feoglobal
feoparameter	Configuration for FEO parameter
feopolicy	Configuration for Front end optimization policy
feopolicy_binding	Binding object showing the resources that can be bound to feopolicy
feopolicy_csvserver_binding	Binding object showing the csvserver that can be bound to feopolicy
feopolicy_feoglobal_binding	Binding object showing the feoglobal that can be bound to feopolicy
feopolicy_lbvserver_binding	Binding object showing the lbvserver that can be bound to feopolicy

feoaction

Configuration for Front end optimization action resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	The name of the front end optimization action. Minimum length = 1
pageextendcache	<Boolean>	Read-write	Extend the time period during which the browser can use the cached resource.
cachemaxage	<Integer>	Read-write	Maxage for cache extension. Default value: 30 Minimum value = 0 Maximum value = 360
imgshrinktoattrib	<Boolean>	Read-write	Shrink image dimensions as per the height and width attributes specified in the <img> tag.
imggiftopng	<Boolean>	Read-write	Convert GIF image formats to PNG formats.
imgtowebp	<Boolean>	Read-write	Convert JPEG, GIF, PNG image formats to WEBP format.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
imgtojpegxr	<Boolean>	Read-write	Convert JPEG, GIF, PNG image formats to JXR format.
imginline	<Boolean>	Read-write	Inline images whose size is less than 2KB.
cssimginline	<Boolean>	Read-write	Inline small images (less than 2KB) referred within CSS files as background-URLs.
jpgoptimize	<Boolean>	Read-write	Remove non-image data such as comments from JPEG images.
imglazyload	<Boolean>	Read-write	Download images, only when the user scrolls the page to view them.
cssminify	<Boolean>	Read-write	Remove comments and whitespaces from CSSs.
cssinline	<Boolean>	Read-write	Inline CSS files, whose size is less than 2KB, within the main page.
csscombine	<Boolean>	Read-write	Combine one or more CSS files into one file.
convertimporttolink	<Boolean>	Read-write	Convert CSS import statements to HTML link tags.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
jsminify	<Boolean>	Read-write	Remove comments and whitespaces from JavaScript.
jsinline	<Boolean>	Read-write	Convert linked JavaScript files (less than 2KB) to inline JavaScript files.
htmlminify	<Boolean>	Read-write	Remove comments and whitespaces from an HTML page.
cssmovetohead	<Boolean>	Read-write	Move any CSS file present within the body tag of an HTML page to the head tag.
jsmovetoend	<Boolean>	Read-write	Move any JavaScript present in the body tag to the end of the body tag.
domainsharding	<String>	Read-write	Domain name of the server.
dnsshards	<String[]>	Read-write	Set of domain names that replaces the parent domain.
clientsidemeasurements	<Boolean>	Read-write	Send AppFlow records about the web pages optimized by this action. The records provide FEO statistics, such as the number of HTTP requests that have been reduced for this page. You must enable the Appflow

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			feature before enabling this parameter.
imgadddimensions	<Boolean>	Read-only	Add dimension attributes to images, if not specified within the <img> tag.
imgshrinkformobile	<Boolean>	Read-only	Serve smaller images for mobile users.
imgweaken	<Boolean>	Read-only	Reduce the image quality.
jpgprogressive	<Boolean>	Read-only	Convert JPEG image formats to progressive formats.
cssflattenimports	<Boolean>	Read-only	Replace CSS import statements with the file content.
jscombine	<Boolean>	Read-only	Combine one or more JavaScript files into one file.
htmlrmdefaultattribs	<Boolean>	Read-only	Remove default redundant attributes from an HTML file.
htmlrmattribquotes	<Boolean>	Read-only	Remove unnecessary quotes present within the HTML attributes.
htmltrimurls	<Boolean>	Read-only	Trim URLs.
hits	<Integer>	Read-only	The number of times the action has been taken.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
undefhits	<Integer>	Read-only	Total number of undefined policy hits.
builtin	<String[]>	Read-only	Flag to determine if front end optimization action is built-in or not. Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL
feature	<String>	Read-only	The feature to be checked while applying this config.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- UPDATE
- UNSET
- DELETE
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/feoaction **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"feoaction":{

<b>"name":<String_value>,

</b>"pageextendcache":<Boolean_value>,

"cachemaxage":<Integer_value>,

"imgshrinktoattrib":<Boolean_value>,

"imggiftopng":<Boolean_value>,
```

```
"imgtowebp":<Boolean_value>,

"imgtojpegxr":<Boolean_value>,

"imginline":<Boolean_value>,

"cssimginline":<Boolean_value>,

"jpgoptimize":<Boolean_value>,

"imglazyload":<Boolean_value>,

"cssminify":<Boolean_value>,

"cssinline":<Boolean_value>,

"csscombine":<Boolean_value>,

"convertimporttolink":<Boolean_value>,

"jsminify":<Boolean_value>,

"jsinline":<Boolean_value>,

"htmlminify":<Boolean_value>,

"cssmovetohead":<Boolean_value>,

"jsmovetoend":<Boolean_value>,

"domainsharding":<String_value>,

"dnsshards":<String[]_value>,

"clientsidemeasurements":<Boolean_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/feoaction **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"feoaction":{

<b>"name":<String_value>,

</b>"pageextendcache":<Boolean_value>,

"cachemaxage":<Integer_value>,

"imgshrinktoattrib":<Boolean_value>,

"imggiftopng":<Boolean_value>,

"imgtowebp":<Boolean_value>,

"imgtojpegxr":<Boolean_value>,

"imginline":<Boolean_value>,

"cssimginline":<Boolean_value>,

"jpgoptimize":<Boolean_value>,

"imglazyload":<Boolean_value>,

"cssminify":<Boolean_value>,

"cssinline":<Boolean_value>,

"csscombine":<Boolean_value>,
```

```
"convertimporttolink":<Boolean_value>,

"jsminify":<Boolean_value>,

"jsinline":<Boolean_value>,

"htmlminify":<Boolean_value>,

"cssmovetohead":<Boolean_value>,

"jsmovetoend":<Boolean_value>,

"domainsharding":<String_value>,

"dnsshards":<String[]_value>,

"clientsidemeasurements":<Boolean_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/feoaction? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"feoaction":{

<b>"name":<String_value>,
```

```
</b>"pageextendcache":true,

"imgshrinktoattrib":true,

"imggiftopng":true,

"imgtowebp":true,

"imgtojpegxr":true,

"imginline":true,

"cssimginline":true,

"jpgoptimize":true,

"imglazyload":true,

"cssminify":true,

"cssinline":true,

"csscombine":true,

"convertimporttolink":true,

"jsminify":true,

"jsinline":true,

"htmlminify":true,

"cssmovetohead":true,

"jsmovetoend":true,

"clientsidemeasurements":true,

"domainsharding":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/feoaction/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/feoaction **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/feoaction? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/feoaction? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of feoaction resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/feoaction? **view=summary**

Use this query-parameter to get the summary output of feoaction resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/feoaction? **pagesize=#no;pageno=#no**

Use this query-parameter to get the feoaction resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "feoaction": [ {

"name":<String_value>,

"pageextendcache":<Boolean_value>,

"cachemaxage":<Integer_value>,

"imgshrinktoattrib":<Boolean_value>,

"imggiftopng":<Boolean_value>,

"imgtowebp":<Boolean_value>,

"imgtojpegxr":<Boolean_value>,

"imgadddimensions":<Boolean_value>,

"imgshrinkformobile":<Boolean_value>,

"imgweaken":<Boolean_value>,

"imginline":<Boolean_value>,

"cssimginline":<Boolean_value>,

"jpgoptimize":<Boolean_value>,
```

```
"jpgprogressive":<Boolean_value>,

"imglazyload":<Boolean_value>,

"cssminify":<Boolean_value>,

"cssinline":<Boolean_value>,

"csscombine":<Boolean_value>,

"cssflattenimports":<Boolean_value>,

"convertimporttolink":<Boolean_value>,

"jsminify":<Boolean_value>,

"jsinline":<Boolean_value>,

"jscombine":<Boolean_value>,

"htmlminify":<Boolean_value>,

"htmlrmdefaultattribs":<Boolean_value>,

"htmlrmattribquotes":<Boolean_value>,

"htmltrimurls":<Boolean_value>,

"cssmovetohead":<Boolean_value>,

"jsmovetoend":<Boolean_value>,

"domainsharding":<String_value>,

"dnsshards":<String[]_value>,

"clientsidemeasurements":<Boolean_value>,

"hits":<Integer_value>,

"undefhits":<Integer_value>,

"builtin":<String[]_value>,
```

```
"feature":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/feoaction/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/feoaction/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/feoaction/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of feoaction resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "feoaction": [ {

"name":<String_value>,

"pageextendcache":<Boolean_value>,

"cachemaxage":<Integer_value>,

"imgshrinktoattrib":<Boolean_value>,

"imggiftopng":<Boolean_value>,

"imgtowebp":<Boolean_value>,

"imgtojpegxr":<Boolean_value>,

"imgadddimensions":<Boolean_value>,

"imgshrinkformobile":<Boolean_value>,

"imgweaken":<Boolean_value>,

"imginline":<Boolean_value>,

"cssimginline":<Boolean_value>,

"jpgoptimize":<Boolean_value>,

"jpgprogressive":<Boolean_value>,

"imglazyload":<Boolean_value>,

"cssminify":<Boolean_value>,

"cssinline":<Boolean_value>,

"csscombine":<Boolean_value>,

"cssflattenimports":<Boolean_value>,

"convertimporttolink":<Boolean_value>,

"jsminify":<Boolean_value>,
```

```
"jsinline":<Boolean_value>,

"jscombine":<Boolean_value>,

"htmlminify":<Boolean_value>,

"htmlrmdefaultattribs":<Boolean_value>,

"htmlrmattribquotes":<Boolean_value>,

"htmltrimurls":<Boolean_value>,

"cssmovetohead":<Boolean_value>,

"jsmovetoend":<Boolean_value>,

"domainsharding":<String_value>,

"dnsshards":<String[]_value>,

"clientsidemeasurements":<Boolean_value>,

"hits":<Integer_value>,

"undefhits":<Integer_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/feoaction? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "feoaction": [ { "__count": "#no"} ] }
```

feoglobal_binding

Binding object which returns the resources bound to feoglobal.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
feoglobal_feopolicy_binding	<feoglobal_feopolicy_binding[]>	Read-write	feopolicy that can be bound to feoglobal.

Operations

(click to see Properties)

- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/feoglobal_binding

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "feoglobal_binding": [ {

"feoglobal_feopolicy_binding":<feoglobal_feopolicy_binding[]_value>
```

```
}]}
```

feoglobal_feopolicy_binding

Binding object showing the feopolicy that can be bound to feoglobal.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
type	<String>	Read-write	Bindpoint to which the policy is bound. Possible values = REQ_OVERRIDE, REQ_DEFAULT, RES_OVERRIDE, RES_DEFAULT, HTTPQUIC_REQ_OVERRIDE, HTTPQUIC_REQ_DEFAULT
policyname	<String>	Read-write	The name of the globally bound front end optimization policy.
globalbindtype	<String>	Read-write	. Default value: SYSTEM_GLOBAL Possible values = SYSTEM_GLOBAL, VPN_GLOBAL, RNAT_GLOBAL,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			APPFW_GLOBAL, TM_GLOBAL
gotopriorityexpression	<String>	Read-write	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
priority	<Integer>	Read-write	The priority assigned to the policy binding.
numpol	<Integer>	Read-only	The number of policies bound to the bindpoint.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/feoglobal_feopolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"feoglobal_feopolicy_binding":{

<b>"policyname":<String_value>,

</b><b>"priority":<Integer_value>,

</b>"type":<String_value>,

"gotopriorityexpression":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/feoglobal_feopolicy_binding **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/feoglobal_feopolicy_binding? **args= policyname:<String_value>, type: <String_value> ,priority: <Integer_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/feoglobal_feopolicy_binding **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/feoglobal_feopolicy_binding? **args=type: <String_value>**

Use this query-parameter to get feoglobal_feopolicy_binding resources based on additional properties.

filter http:// <netscaler-ip-address> /nitro/v1/config/feoglobal_feopolicy_binding? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of feoglobal_feopolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/feoglobal_feopolicy_binding? **pagesize=#no;pageno=#no**

Use this query-parameter to get the feoglobal_feopolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "feoglobal_feopolicy_binding": [ {

"type":<String_value>,

"policyname":<String_value>,

"globalbindtype":<String_value>,

"gotopriorityexpression":<String_value>,

"priority":<Integer_value>,

"numpol":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/feoglobal_feopolicy_binding? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "feoglobal_feopolicy_binding": [ { "__count": "#no"} ] }
```

feoparameter

Configuration for FEO parameter resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
jpegqualitypercent	<Integer>	Read-write	The percentage value of a JPEG image quality to be reduced. Range: 0 - 100. Default value: 75 Minimum value = 0 Maximum value = 100
cssinlinethressize	<Integer>	Read-write	Threshold value of the file size (in bytes) for converting external CSS files to inline CSS files. Default value: 1024 Minimum value = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum value = 2048
jsinlinethressize	<Integer>	Read-write	Threshold value of the file size (in bytes), for converting external JavaScript files to inline JavaScript files. Default value: 1024 Minimum value = 1 Maximum value = 2048
imginlinethressize	<Integer>	Read-write	Maximum file size of an image (in bytes), for coverting linked images to inline images. Default value: 1024 Minimum value = 1 Maximum value = 2048
builtin	<String[]>	Read-only	Specify the builtin flags for - set feo param. Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL
feature	<String>	Read-only	The feature to be checked while applying this config.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- UPDATE
- UNSET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/feoparameter **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"feoparameter":{

"jpegqualitypercent":<Integer_value>,

"cssinlinethressize":<Integer_value>,

"jsinlinethressize":<Integer_value>,

"imginlinethressize":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/feoparameter? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"feoparameter":{

"jpegqualitypercent":true,

"cssinlinethressize":true,
```

```
"jsinlinethressize":true,

"imginlinethressize":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/feoparameter **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "feoparameter": [ {

"jpegqualitypercent":<Integer_value>,

"cssinlinethressize":<Integer_value>,

"jsinlinethressize":<Integer_value>,

"imginlinethressize":<Integer_value>,

"builtin":<String[]_value>,
```

```
"feature":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

feopolicy

Configuration for Front end optimization policy resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	The name of the front end optimization policy. Minimum length = 1
rule	<String>	Read-write	The rule associated with the front end optimization policy.
action	<String>	Read-write	The front end optimization action that has to be performed when the rule matches. Minimum length = 1
builtin	<String[]>	Read-only	Flag to determine if the front end optimization policy is built-in or not. Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
feature	<String>	Read-only	The feature to be checked while applying this config.
hits	<Integer>	Read-only	Total number of hits.
undefhits	<Integer>	Read-only	Total number of undefined policy hits.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of

creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/feopolicy **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"feopolicy":{

<b>"name":<String_value>,

</b><b>"rule":<String_value>,

</b><b>"action":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/feopolicy/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/feopolicy **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"feopolicy":{

<b>"name":<String_value>,

</b>"rule":<String_value>,

"action":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/feopolicy? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"feopolicy":{

<b>"name":<String_value>,

</b>"rule":true,

"action":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/feopolicy **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/feopolicy? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/feopolicy? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of feopolicy resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/feopolicy? **view=summary**

Use this query-parameter to get the summary output of feopolicy resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/feopolicy? **pagesize=#no;pageno=#no**

Use this query-parameter to get the feopolicy resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "feopolicy": [ {

"name":<String_value>,

"rule":<String_value>,

"action":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"hits":<Integer_value>,

"undefhits":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/feopolicy/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/feopolicy/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/feopolicy/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of feopolicy resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "feopolicy": [ {

"name":<String_value>,

"rule":<String_value>,

"action":<String_value>,

"builtin":<String[]_value>,
```

```
"feature":<String_value>,

"hits":<Integer_value>,

"undefhits":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/feopolicy? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "feopolicy": [ { "__count": "#no"} ] }
```

feopolicy_binding

Binding object which returns the resources bound to feopolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	The name of the front end optimization policy. Minimum length = 1
feopolicy_lbvserver_binding	<feopolicy_lbvserver_binding[]>	Read-only	lbvserver that can be bound to feopolicy.
feopolicy_csvserver_binding	<feopolicy_csvserver_binding[]>	Read-only	csvserver that can be bound to feopolicy.
feopolicy_feoglobal_binding	<feopolicy_feoglobal_binding[]>	Read-only	feoglobal that can be bound to feopolicy.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/feopolicy_binding/ name_value<String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "feopolicy_binding": [ {

"name":<String_value>,

"feopolicy_lbvserver_binding":<feopolicy_lbvserver_binding[]_value>,

"feopolicy_csvserver_binding":<feopolicy_csvserver_binding[]_value>,

"feopolicy_feoglobal_binding":<feopolicy_feoglobal_binding[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/feopolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/feopolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "feopolicy_binding": [ {

"name":<String_value>,

"feopolicy_lbvserver_binding":<feopolicy_lbvserver_binding[]_value>,

"feopolicy_csvserver_binding":<feopolicy_csvserver_binding[]_value>,

"feopolicy_feoglobal_binding":<feopolicy_feoglobal_binding[]_value>

}]}
```

feopolicy_csvserver_binding

Binding object showing the csvserver that can be bound to feopolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
boundto	<String>	Read-write	Location where the policy is bound to.
name	<String>	Read-write	The name of the front end optimization policy. Minimum length = 1
activepolicy	<Integer>	Read-only	Indicates whether a policy is bound or not.
gotopriorityexpression	<String>	Read-only	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
priority	<Integer>	Read-only	Priority of the policy.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/feopolicy_csvserver_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ feopolicy_csvserver_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of feopolicy_csvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/feopolicy_csvserver_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the feopolicy_csvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "feopolicy_csvserver_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"activepolicy":<Integer_value>,

"gotopriorityexpression":<String_value>,

"priority":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/feopolicy_csvserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/feopolicy_csvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "feopolicy_csvserver_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"activepolicy":<Integer_value>,

"gotopriorityexpression":<String_value>,

"priority":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/feopolicy_csvserver_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"feopolicy_csvserver_binding": [ { "__count": "#no"} ] }
```

feopolicy_feoglobal_binding

Binding object showing the feoglobal that can be bound to feopolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	The name of the front end optimization policy. Minimum length = 1
boundto	<String>	Read-write	Location where the policy is bound to.
priority	<Integer>	Read-only	Priority of the policy.
gotopriorityexpression	<String>	Read-only	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
activepolicy	<Integer>	Read-only	Indicates whether a policy is bound or not.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)

- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/feopolicy_feoglobal_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ feopolicy_feoglobal_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of feopolicy_feoglobal_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/feopolicy_feoglobal_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the feopolicy_feoglobal_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "feopolicy_feoglobal_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"priority":<Integer_value>,

"gotopriorityexpression":<String_value>,

"activepolicy":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/feopolicy_feoglobal_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/feopolicy_feoglobal_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "feopolicy_feoglobal_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"priority":<Integer_value>,

"gotopriorityexpression":<String_value>,

"activepolicy":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/feopolicy_feoglobal_binding/name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"feopolicy_feoglobal_binding": [ { "__count": "#no"} ] }
```

feopolicy_lbvserver_binding

Binding object showing the lbvserver that can be bound to feopolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
boundto	<String>	Read-write	Location where the policy is bound to.
name	<String>	Read-write	The name of the front end optimization policy. Minimum length = 1
priority	<Integer>	Read-only	Priority of the policy.
activepolicy	<Integer>	Read-only	Indicates whether a policy is bound or not.
gotopriorityexpression	<String>	Read-only	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/feopolicy_lbvserver_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ feopolicy_lbvserver_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of feopolicy_lbvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/feopolicy_lbvserver_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the feopolicy_lbvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "feopolicy_lbvserver_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"priority":<Integer_value>,

"activepolicy":<Integer_value>,

"gotopriorityexpression":<String_value>
```

```
}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/feopolicy_lbvserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/feopolicy_lbvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "feopolicy_lbvserver_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"priority":<Integer_value>,

"activepolicy":<Integer_value>,

"gotopriorityexpression":<String_value>
```

```
}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/feopolicy_lbvserver_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"feopolicy_lbvserver_binding": [ { "__count": "#no"} ] }
```

gslb

Global Server Load Balancing

Global Server Load Balancing (GSLB) configuration. GSLB feature ensures that client requests are directed to a best performing site available in a global enterprise and distributed Internet environment.

NAME	DESCRIPTION
gslbconfig	Configuration for gslb config
gslbdomain	Configuration for GSLB domain

NAME	DESCRIPTION
gslbdomain_binding	Binding object showing the resources that can be bound to gslbdomain
gslbdomain_gslbservice_binding	Binding object showing the gslbservice that can be bound to gslbdomain
gslbdomain_gslbservicegroup_binding	Binding object showing the gslbservicegroup that can be bound to gslbdomain
gslbdomain_gslbservicegroupmember_binding	Binding object showing the gslbservicegroupmember that can be bound to gslbdomain
gslbdomain_gslbvserver_binding	Binding object showing the gslbvserver that can be bound to gslbdomain
gslbdomain_lbmonitor_binding	Binding object showing the lbmonitor that can be bound to gslbdomain
gslbldnsentries	Configuration for LDNS entry
gslbldnsentry	Configuration for LDNS entry
gslbparameter	Configuration for GSLB parameter
gslbrunningconfig	Configuration for running GSLB configuration
gslbservice	Configuration for GSLB service

NAME	DESCRIPTION
gslbservice_binding	Binding object showing the resources that can be bound to gslbservice
gslbservice_dnsview_binding	Binding object showing the dnsview that can be bound to gslbservice
gslbservice_lbmonitor_binding	Binding object showing the lbmonitor that can be bound to gslbservice
gslbservicegroup	Configuration for GSLB service group
gslbservicegroup_binding	Binding object showing the resources that can be bound to gslbservicegroup
gslbservicegroup_gslbservicegroupmember_binding	Binding object showing the gslbservicegroupmember that can be bound to gslbservicegroup
gslbservicegroup_lbmonitor_binding	Binding object showing the lbmonitor that can be bound to gslbservicegroup
gslbservicegroup_servicegroupentitymonbindings_binding	Binding object showing the servicegroupentitymonbindings that can be bound to gslbservicegroup
gslbsite	Configuration for GSLB site
gslbsite_binding	Binding object showing the resources that can be bound to gslbsite

NAME	DESCRIPTION
gslbsite_gslbservice_binding	Binding object showing the gslbservice that can be bound to gslbsite
gslbsite_gslbservicegroup_binding	Binding object showing the gslbservicegroup that can be bound to gslbsite
gslbsite_gslbservicegroupmember_binding	Binding object showing the gslbservicegroupmember that can be bound to gslbsite
gslbsyncstatus	Configuration for sync status
gslbvserver	Configuration for Global Server Load Balancing Virtual Server
gslbvserver_binding	Binding object showing the resources that can be bound to gslbvserver
gslbvserver_domain_binding	Binding object showing the domain that can be bound to gslbvserver
gslbvserver_gslbservice_binding	Binding object showing the gslbservice that can be bound to gslbvserver
gslbvserver_gslbservicegroup_binding	Binding object showing the gslbservicegroup that can be bound to gslbvserver
gslbvserver_gslbservicegroupmember_binding	Binding object showing the gslbservicegroupmember that can be bound to gslbvserver

NAME	DESCRIPTION
gslbvserver_lbpolicy_binding	Binding object showing the lbpolicy that can be bound to gslbvserver
gslbvserver_spilloverpolicy_binding	Binding object showing the spilloverpolicy that can be bound to gslbvserver

gslbconfig

Configuration for gslb config resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
preview	<Boolean>	Read-write	Do not synchronize the GSLB sites, but display the commands that would be applied on the slave node upon synchronization. Mutually exclusive with the Save Configuration option.
debug	<Boolean>	Read-write	Generate verbose output when synchronizing the GSLB sites. The Debug option generates more verbose output than the sync gslb config command in which the option is not used, and is useful for analyzing

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			synchronization issues.
forcesync	<String>	Read-write	Force synchronization of the specified site even if a dependent configuration on the remote site is preventing synchronization or if one or more GSLB entities on the remote site have the same name but are of a different type. You can specify either the name of the remote site that you want to synchronize with the local site, or you can specify All Sites in the configuration utility (the string all-sites in the CLI). If you specify All Sites, all the sites in the GSLB setup are synchronized with the site on the master node. Note: If you select the Force Sync option, the synchronization starts without displaying the commands that are

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			going to be executed.
nowarn	<Boolean>	Read-write	Suppress the warning and the confirmation prompt that are displayed before site synchronization begins. This option can be used in automation scripts that must not be interrupted by a prompt.
saveconfig	<Boolean>	Read-write	Save the configuration on all the nodes participating in the synchronization process, automatically. The master saves its configuration immediately before synchronization begins. Slave nodes save their configurations after the process of synchronization is complete. A slave node saves its configuration only if the configuration difference was successfully applied to it. Mutually

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			exclusive with the Preview option.
command	<String>	Read-write	Run the specified command on the master node and then on all the slave nodes. You cannot use this option with the force sync and preview options.

Operations

(click to see Properties)

- SYNC

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

SYNC

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbconfig? **action=sync HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"gslbconfig":{

"preview":<Boolean_value>,

"debug":<Boolean_value>,

"forcesync":<String_value>,

"nowarn":<Boolean_value>,

"saveconfig":<Boolean_value>,

"command":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

gslbdomain

Configuration for GSLB domain resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the Domain. Minimum length = 1
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbdomain **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/gslbdomain? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/gslbdomain? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of gslbdomain resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/gslbdomain? **view=summary**

Use this query-parameter to get the summary output of gslbdomain resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/gslbdomain? **pagesize=#no;pageno=#no**

Use this query-parameter to get the gslbdomain resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "gslbdomain": [ {

"name":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbdomain/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/gslbdomain/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/gslbdomain/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of gslbdomain resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "gslbdomain": [ {

"name":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbdomain? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "gslbdomain": [ { "__count": "#no"} ] }
```

gslbdomain_binding

Binding object which returns the resources bound to gslbdomain.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the Domain.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum length = 1
gslbdomain_gslbvserver_binding	<gslbdomain_gslbvserver_binding[]>	Read-only	gslbvserver that can be bound to gslbdomain.
gslbdomain_gslbservicegroupmember_binding	<gslbdomain_gslbservicegroupmember_binding[]>	Read-only	gslbservicegroupmember that can be bound to gslbdomain.
gslbdomain_gslbservice_binding	<gslbdomain_gslbservice_binding[]>	Read-only	gslbservice that can be bound to gslbdomain.
gslbdomain_lbmonitor_binding	<gslbdomain_lbmonitor_binding[]>	Read-only	lbmonitor that can be bound to gslbdomain.
gslbdomain_gslbservicegroup_binding	<gslbdomain_gslbservicegroup_binding[]>	Read-only	gslbservicegroup that can be bound to gslbdomain.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbdomain_binding/ name_value<String>
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "gslbdomain_binding": [ {

"name":<String_value>,

"gslbdomain_gslbservicegroupmember_binding":<gslbdomain_gslbservicegroupme
mber_binding[]_value>,
```

```
"gslbdomain_gslbservice_binding":<gslbdomain_gslbservice_binding[]_value>,

"gslbdomain_gslbservicegroup_binding":<gslbdomain_gslbservicegroup_binding
[]_value>,

"gslbdomain_lbmonitor_binding":<gslbdomain_lbmonitor_binding[]_value>,

"gslbdomain_gslbvserver_binding":<gslbdomain_gslbvserver_binding[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbdomain_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/gslbdomain_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "gslbdomain_binding": [ {

"name":<String_value>,
```

```
"gslbdomain_gslbservicegroupmember_binding":<gslbdomain_gslbservicegroupme
mber_binding[]_value>,

"gslbdomain_gslbservice_binding":<gslbdomain_gslbservice_binding[]_value>,

"gslbdomain_gslbservicegroup_binding":<gslbdomain_gslbservicegroup_binding
[]_value>,

"gslbdomain_lbmonitor_binding":<gslbdomain_lbmonitor_binding[]_value>,

"gslbdomain_gslbvserver_binding":<gslbdomain_gslbvserver_binding[]_value>

}]}
```

gslbdomain_gslbservice_binding

Binding object showing the gslbservice that can be bound to gslbdomain.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the Domain. Minimum length = 1
servicename	<String>	Read-write	The service name.
cumulativeweight	<Integer>	Read-only	cumlative weight.
port	<Integer>	Read-only	Port Number. Minimum value = 1 Range 1 - 65535 * in CLI is represented as 65535 in NITRO API

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
servicetype	<String>	Read-only	The type GSLB service. Possible values = HTTP, FTP, TCP, UDP, SSL, SSL_BRIDGE, SSL_TCP, NNTP, ANY, SIP_UDP, SIP_TCP, SIP_SSL, RADIUS, RDP, RTSP, MYSQL, MSSQL, ORACLE
ipaddress	<String>	Read-only	The Ip address of the service.
order	<Integer>	Read-only	Order number assigned to the service when it is bound to the gslb vserver.
cnameentry	<String>	Read-only	The cname of the gslb service.
state	<String>	Read-only	The state of the vserver. Possible values = UP, DOWN, UNKNOWN, BUSY, OUT OF SERVICE, GOING OUT OF SERVICE, DOWN WHEN GOING OUT OF SERVICE, NS_EMPTY_STR, Unknown, DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
weight	<Integer>	Read-only	weight assigned. Minimum value = 1 Maximum value = 100
dynamicconfwt	<Integer>	Read-only	dynamic weight.
svreffgslbstate	<String>	Read-only	GSLB server state. Possible values = UP, DOWN, UNKNOWN, BUSY, OUT OF SERVICE, GOING OUT OF SERVICE, DOWN WHEN GOING OUT OF SERVICE, NS_EMPTY_STR, Unknown, DISABLED
vservername	<String>	Read-only	.
gslbthreshold	<Integer>	Read-only	The threshold value of the service.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbdomain_gslbservice_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ gslbdomain_gslbservice_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of gslbdomain_gslbservice_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/gslbdomain_gslbservice_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the gslbdomain_gslbservice_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "gslbdomain_gslbservice_binding": [ {

"name":<String_value>,

"servicename":<String_value>,

"cumulativeweight":<Integer_value>,

"port":<Integer_value>,

"servicetype":<String_value>,

"ipaddress":<String_value>,

"order":<Integer_value>,

"cnameentry":<String_value>,

"state":<String_value>,

"weight":<Integer_value>,

"dynamicconfwt":<Integer_value>,

"svreffgslbstate":<String_value>,

"vservername":<String_value>,

"gslbthreshold":<Integer_value>
```

```
}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbdomain_gslbservice_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/gslbdomain_gslbservice_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "gslbdomain_gslbservice_binding": [ {

"name":<String_value>,

"servicename":<String_value>,

"cumulativeweight":<Integer_value>,

"port":<Integer_value>,

"servicetype":<String_value>,
```

```
"ipaddress":<String_value>,

"order":<Integer_value>,

"cnameentry":<String_value>,

"state":<String_value>,

"weight":<Integer_value>,

"dynamicconfwt":<Integer_value>,

"svreffgslbstate":<String_value>,

"vservername":<String_value>,

"gslbthreshold":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbdomain_gslbservice_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"gslbdomain_gslbservice_binding": [ { "__count": "#no"} ] }
```

gslbdomain_gslbservicegroup_binding

Binding object showing the gslbservicegroup that can be bound to gslbdomain.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
servicegroupname	<String>	Read-write	The GSLB service group name bound to the selected GSLB virtual server.
name	<String>	Read-write	Name of the Domain. Minimum length = 1
order	<Integer>	Read-only	Order number assigned to the service when it is bound to the gslb vserver.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbdomain_gslbservicegroup_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ gslbdomain_gslbservicegroup_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of gslbdomain_gslbservicegroup_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/gslbdomain_gslbservicegroup_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the gslbdomain_gslbservicegroup_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "gslbdomain_gslbservicegroup_binding": [ {

"servicegroupname":<String_value>,

"name":<String_value>,

"order":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbdomain_gslbservicegroup_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/gslbdomain_gslbservicegroup_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "gslbdomain_gslbservicegroup_binding": [ {

"servicegroupname":<String_value>,

"name":<String_value>,

"order":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbdomain_gslbservicegroup_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"gslbdomain_gslbservicegroup_binding": [ { "__count": "#no"} ] }
```

gslbdomain_gslbservicegroupmember_binding

Binding object showing the gslbservicegroupmember that can be bound to gslbdomain.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
servicegroupname	<String>	Read-write	The GSLB service group name bound to the selected GSLB virtual server.
name	<String>	Read-write	Name of the Domain. Minimum length = 1
order	<Integer>	Read-only	Order number assigned to the service when it is bound to the gslb vserver.
gslbthreshold	<Integer>	Read-only	The threshold value of the service.
servicetype	<String>	Read-only	The type GSLB service. Possible values = HTTP, FTP, TCP, UDP, SSL, SSL_BRIDGE, SSL_TCP, NNTP, ANY, SIP_UDP, SIP_TCP, SIP_SSL, RADIUS, RDP, RTSP, MYSQL, MSSQL, ORACLE
port	<Integer>	Read-only	Port Number. Minimum value = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Range 1 - 65535 * in CLI is represented as 65535 in NITRO API
ipaddress	<String>	Read-only	The Ip address of the service.
weight	<Integer>	Read-only	weight assigned. Minimum value = 1 Maximum value = 100
svreffgslbstate	<String>	Read-only	GSLB server state. Possible values = UP, DOWN, UNKNOWN, BUSY, OUT OF SERVICE, GOING OUT OF SERVICE, DOWN WHEN GOING OUT OF SERVICE, NS_EMPTY_STR, Unknown, DISABLED
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbdomain_gslbservicegroupmember_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ gslbdomain_gslbservicegroupmember_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of gslbdomain_gslbservicegroupmember_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ gslbdomain_gslbservicegroupmember_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the gslbdomain_gslbservicegroupmember_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "gslbdomain_gslbservicegroupmember_binding": [ {

"servicegroupname":<String_value>,

"name":<String_value>,

"order":<Integer_value>,

"gslbthreshold":<Integer_value>,

"servicetype":<String_value>,

"port":<Integer_value>,

"ipaddress":<String_value>,

"weight":<Integer_value>,

"svreffgslbstate":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbdomain_gslbservicegroupmember_binding
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/gslbdomain_gslbservicegroupmember_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "gslbdomain_gslbservicegroupmember_binding": [ {

"servicegroupname":<String_value>,

"name":<String_value>,

"order":<Integer_value>,

"gslbthreshold":<Integer_value>,

"servicetype":<String_value>,

"port":<Integer_value>,

"ipaddress":<String_value>,
```

```
"weight":<Integer_value>,

"svreffgslbstate":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbdomain_gslbservicegroupmember_binding/name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"gslbdomain_gslbservicegroupmember_binding": [ { "__count": "#no"} ] }
```

gslbdomain_gslbvserver_binding

Binding object showing the gslbvserver that can be bound to gslbdomain.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the Domain. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
vservername	<String>	Read-write	.
sitename	<String>	Read-only	Name of the site to which the service belongs.
persistmask	<String>	Read-only	The optional IPv4 network mask applied to IPv4 addresses to establish source IP address based persistence. Minimum length = 1
persistenceid	<Integer>	Read-only	Persistence id of the gslb vserver.
dnsrecordtype	<String>	Read-only	The IP type for this GSLB vserver. Possible values = A, AAAA, CNAME, NAPTR
v6netmasklen	<Integer>	Read-only	Number of bits to consider, in an IPv6 source IP address, for creating the hash that is required by the SOURCEIPHASH load balancing method. Default value: 128 Minimum value = 1 Maximum value = 128

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
dynamicweight	<String>	Read-only	Dynamic weight method of the vserver. Default value: DISABLED Possible values = SERVICECOUNT, SERVICEWEIGHT, DISABLED
customheaders	<String>	Read-only	The string that is sent to the service. Applicable to HTTP ,HTTP-ECV and RTSP monitor types.
statechangetimesec	<String>	Read-only	Time since last state change.
persistencetype	<String>	Read-only	Indicates if persistence is set on the gslb vserver. Possible values = SOURCEIP, NONE
edr	<String>	Read-only	Send clients an empty DNS response when the GSLB virtual server is DOWN. Default value: DISABLED Possible values = ENABLED, DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
lbmethod	<String>	Read-only	The load balancing method set for the virtual server. Possible values = ROUNDROBIN, LEASTCONNECTION, LEASTRESPONSETIME, SOURCEIPHASH, LEASTBANDWIDTH, LEASTPACKETS, STATICPROXIMITY, RTT, CUSTOMLOAD, API
state	<String>	Read-only	The state of the vserver. Possible values = UP, DOWN, UNKNOWN, BUSY, OUT OF SERVICE, GOING OUT OF SERVICE, DOWN WHEN GOING OUT OF SERVICE, NS_EMPTY_STR, Unknown, DISABLED
netmask	<String>	Read-only	Netmask. Minimum length = 1
cip	<String>	Read-only	Indicates if Client IP option is enabled.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ENABLED, DISABLED
siteprefix	<String>	Read-only	The site prefix string.
v6persistmasklen	<Integer>	Read-only	Number of bits to consider in an IPv6 source IP address when creating source IP address based persistence sessions. Default value: 128 Minimum value = 1 Maximum value = 128
sitepersistence	<String>	Read-only	Indicates the type of cookie persistence set. Possible values = ConnectionProxy, HTTPRedirect, NONE
mir	<String>	Read-only	. Default value: DISABLED Possible values = ENABLED, DISABLED
servicetype	<String>	Read-only	The type GSLB service. Possible values = HTTP, FTP, TCP,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			UDP, SSL, SSL_BRIDGE, SSL_TCP, NNTP, ANY, SIP_UDP, SIP_TCP, SIP_SSL, RADIUS, RDP, RTSP, MYSQL, MSSQL, ORACLE
backuplbmethod	<String>	Read-only	Indicates the backup method in case the primary fails. Possible values = ROUNDROBIN, LEASTCONNECTION, LEASTRESPONSETIME, SOURCEIPHASH, LEASTBANDWIDTH, LEASTPACKETS, STATICPROXIMITY, RTT, CUSTOMLOAD, API
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbdomain_gslbvserver_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ gslbdomain_gslbvserver_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of gslbdomain_gslbvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/gslbdomain_gslbvserver_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the gslbdomain_gslbvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "gslbdomain_gslbvserver_binding": [ {

"name":<String_value>,

"vservername":<String_value>,

"sitename":<String_value>,

"persistmask":<String_value>,

"persistenceid":<Integer_value>,

"dnsrecordtype":<String_value>,

"v6netmasklen":<Integer_value>,

"dynamicweight":<String_value>,

"customheaders":<String_value>,

"statechangetimesec":<String_value>,

"persistencetype":<String_value>,

"edr":<String_value>,

"lbmethod":<String_value>,

"state":<String_value>,
```

```
"netmask":<String_value>,

"cip":<String_value>,

"siteprefix":<String_value>,

"v6persistmasklen":<Integer_value>,

"sitepersistence":<String_value>,

"mir":<String_value>,

"servicetype":<String_value>,

"backuplbmethod":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbdomain_gslbvserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/gslbdomain_gslbvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "gslbdomain_gslbvserver_binding": [ {

"name":<String_value>,

"vservername":<String_value>,

"sitename":<String_value>,

"persistmask":<String_value>,

"persistenceid":<Integer_value>,

"dnsrecordtype":<String_value>,

"v6netmasklen":<Integer_value>,

"dynamicweight":<String_value>,

"customheaders":<String_value>,

"statechangetimesec":<String_value>,

"persistencetype":<String_value>,

"edr":<String_value>,

"lbmethod":<String_value>,

"state":<String_value>,

"netmask":<String_value>,

"cip":<String_value>,

"siteprefix":<String_value>,

"v6persistmasklen":<Integer_value>,

"sitepersistence":<String_value>,
```

```
"mir":<String_value>,

"servicetype":<String_value>,

"backuplbmethod":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbdomain_gslbvserver_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"gslbdomain_gslbvserver_binding": [ { "__count": "#no"} ] }
```

gslbdomain_lbmonitor_binding

Binding object showing the lbmonitor that can be bound to gslbdomain.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the Domain. Minimum length = 1
monitorname	<String>	Read-write	Monitor name.
httprequest	<String>	Read-only	HTTP request to the backend server.
monitorcurrentfailedprobes	<Integer>	Read-only	Total number of current failed probes.
vservername	<String>	Read-only	.
responsetime	<Integer>	Read-only	Response time of this monitor.
customheaders	<String>	Read-only	The string that is sent to the service. Applicable to HTTP ,HTTP-ECV and RTSP monitor types.
grpcstatuscode	<Integer>	Read-only	The gRPC status codes.
lastresponse	<String>	Read-only	The string form of monstatcode.
respcode	<String>	Read-only	The response codes.
grpcservicename	<String>	Read-only	The gRPC service name.
iptunnel	<String>	Read-only	The state of the monitor for tunneled devices. Possible values = YES, NO
servicename	<String>	Read-only	The service name.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
grpchealthcheck	<String>	Read-only	The gRPC health check service status. Default value: NO Possible values = YES, NO
monitortotalfailedprobes	<Integer>	Read-only	Total probes failed.
monstatcode	<Integer>	Read-only	The code indicating the monitor response.
monitortotalprobes	<Integer>	Read-only	Total monitor probes.
monstate	<String>	Read-only	Monitor state. Possible values = UP, DOWN, UNKNOWN, BUSY, OUT OF SERVICE, GOING OUT OF SERVICE, DOWN WHEN GOING OUT OF SERVICE, NS_EMPTY_STR, Unknown, DISABLED
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbdomain_lbmonitor_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ gslbdomain_lbmonitor_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of gslbdomain_lbmonitor_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/gslbdomain_lbmonitor_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the gslbdomain_lbmonitor_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "gslbdomain_lbmonitor_binding": [ {

"name":<String_value>,

"monitorname":<String_value>,

"httprequest":<String_value>,

"monitorcurrentfailedprobes":<Integer_value>,

"vservername":<String_value>,

"responsetime":<Integer_value>,

"customheaders":<String_value>,

"grpcstatuscode":<Integer_value>,

"lastresponse":<String_value>,

"respcode":<String_value>,

"grpcservicename":<String_value>,

"iptunnel":<String_value>,

"servicename":<String_value>,
```

```
"grpchealthcheck":<String_value>,

"monitortotalfailedprobes":<Integer_value>,

"monstatcode":<Integer_value>,

"monitortotalprobes":<Integer_value>,

"monstate":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbdomain_lbmonitor_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/gslbdomain_lbmonitor_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "gslbdomain_lbmonitor_binding": [ {

"name":<String_value>,

"monitorname":<String_value>,

"httprequest":<String_value>,

"monitorcurrentfailedprobes":<Integer_value>,

"vservername":<String_value>,

"responsetime":<Integer_value>,

"customheaders":<String_value>,

"grpcstatuscode":<Integer_value>,

"lastresponse":<String_value>,

"respcode":<String_value>,

"grpcservicename":<String_value>,

"iptunnel":<String_value>,

"servicename":<String_value>,

"grpchealthcheck":<String_value>,

"monitortotalfailedprobes":<Integer_value>,

"monstatcode":<Integer_value>,

"monitortotalprobes":<Integer_value>,

"monstate":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbdomain_lbmonitor_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"gslbdomain_lbmonitor_binding": [ { "__count": "#no"} ] }
```

gslbldnsentries

Configuration for LDNS entry resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
nodeid	<Integer>	Read-write	Unique number that identifies the cluster node. Minimum value = 0 Maximum value = 31
sitename	<String>	Read-only	The GSLB site name.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
numsites	<Integer>	Read-only	Specifies the number of gslb sites.
ipaddress	<String>	Read-only	IP address of the LDNS server.
ttl	<Integer>	Read-only	TTL value of the LDNS entry.
name	<String>	Read-only	Monitor that is currently being used to monitor the LDNS ip..
rtt	<Integer[]>	Read-only	RTT value of the LDNS entry for all gslb sites.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- CLEAR
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

CLEAR

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbldnsentries? **action=clear HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"gslbldnsentries":{

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbldnsentries **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/gslbldnsentries? **args=nodeid: <Integer_value>**

Use this query-parameter to get gslbldnsentries resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/config/gslbldnsentries? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/gslbldnsentries? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of gslbldnsentries resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/gslbldnsentries? **view=summary**

Use this query-parameter to get the summary output of gslbldnsentries resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/gslbldnsentries? **pagesize=#no;pageno=#no**

Use this query-parameter to get the gslbldnsentries resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "gslbldnsentries": [ {

nodeid:<Integer_value>"sitename":<String_value>,

"numsites":<Integer_value>,

"ipaddress":<String_value>,

"ttl":<Integer_value>,

"name":<String_value>,

"rtt":<Integer[]_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbldnsentries? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "gslbldnsentries": [ { "__count": "#no"} ] }
```

gslbldnsentry

Configuration for LDNS entry resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ipaddress	<String>	Read-write	IP address of the LDNS server. Minimum length = 1

Operations

(click to see Properties)

- DELETE

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbldnsentry **Query-parameters: args= ipaddress:<String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

gslbparameter

Configuration for GSLB parameter resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ldnsentrytimeout	<Integer>	Read-write	Time, in seconds, after which an inactive LDNS entry is removed. Default value: 180 Minimum value = 30 Maximum value = 65534
rtttolerance	<Integer>	Read-write	Tolerance, in milliseconds, for newly learned round-trip time (RTT) values. If the difference between the old RTT value

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			and the newly computed RTT value is less than or equal to the specified tolerance value, the LDNS entry in the network metric table is not updated with the new RTT value. Prevents the exchange of metrics when variations in RTT values are negligible. Default value: 5 Minimum value = 1 Maximum value = 100
ldnsmask	<String>	Read-write	The IPv4 network mask with which to create LDNS entries. Minimum length = 1
v6ldnsmasklen	<Integer>	Read-write	Mask for creating LDNS entries for IPv6 source addresses. The mask is defined as the number of leading bits to consider, in the source IP address, when creating an LDNS entry. Default value: 128 Minimum value = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum value = 128
ldnsprobeorder	<String[]>	Read-write	Order in which monitors should be initiated to calculate RTT. Possible values = PING, DNS, TCP
dropldnsreq	<String>	Read-write	Drop LDNS requests if round-trip time (RTT) information is not available. Default value: DISABLED Possible values = ENABLED, DISABLED
gslbsvcstatedelaytime	<Integer>	Read-write	Amount of delay in updating the state of GSLB service to DOWN when MEP goes down. This parameter is applicable only if monitors are not bound to GSLB services. Default value: 0 Minimum value = 0 Maximum value = 3600

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
svcstatelearningtime	<Integer>	Read-write	Time (in seconds) within which local or child site services remain in learning phase. GSLB site will enter the learning phase after reboot, HA failover, Cluster GSLB owner node changes or MEP being enabled on local node. Backup parent (if configured) will selectively move the adopted children's GSLB services to learning phase when primary parent goes down. While a service is in learning period, remote site will not honour the state and stats got through MEP for that service. State can be learnt from health monitor if bound explicitly. Default value: 0 Minimum value = 0 Maximum value = 3600
automaticconfigsync	<String>	Read-write	GSLB configuration will be synced automatically to remote gslb sites if enabled.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: DISABLED Possible values = ENABLED, DISABLED
mepkeepalivetimeout	<Integer>	Read-write	Time duartion (in seconds) during which if no new packets received by Local gslb site from Remote gslb site then mark the MEP connection DOWN. Default value: 10 Minimum value = 1
gslbsyncinterval	<Integer>	Read-write	Time duartion (in seconds) for which the gslb sync process will wait before checking for config changes. Default value: 10 Minimum value = 1
gslbsyncmode	<String>	Read-write	Mode in which configuration will be synced from master site to remote sites. Default value: IncrementalSync Possible values = IncrementalSync, FullSync

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
gslbsynclocfiles	<String>	Read-write	If disabled, Location files will not be synced to the remote sites as part of manual sync and automatic sync. Default value: ENABLED Possible values = ENABLED, DISABLED
gslbconfigsyncmonitor	<String>	Read-write	If enabled, remote gslb site's rsync port will be monitored and site is considered for configuration sync only when the monitor is successful. Default value: DISABLED Possible values = ENABLED, DISABLED
gslbsyncsaveconfigcommand	<String>	Read-write	If enabled, 'save ns config' command will be treated as other GSLB commands and synced to GSLB nodes when auto gslb sync option is enabled. Default value: DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ENABLED, DISABLED
undefaction	<String>	Read-write	Action to perform when policy evaluation creates an UNDEF condition. Available settings function as follows: * NOLBACTION - Does not consider LB action in making LB decision. * RESET - Reset the request and notify the user, so that the user can resend the request. * DROP - Drop the request without sending a response to the user. Default value: "NOLBACTION"
usekrpcchannelforsync	<String>	Read-write	This option is to use Krpc channel for GSLB sync. Default value: DISABLED Possible values = ENABLED, DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
sourceipwhitelisting	<String>	Read-write	If enabled, local gslb site private IP would be used as the source IP while initiating MEP/GSLB sync connection if srcIP is not configured for GSLB site. Default value: DISABLED Possible values = ENABLED, DISABLED
flags	<Integer>	Read-only	State of the GSLB parameter.
builtin	<String[]>	Read-only	. Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL
feature	<String>	Read-only	The feature to be checked while applying this config.
incarnation	<Integer>	Read-only	This is a counter to maintain the gslb sync incarnation number.
overridepersistencyfororder	<String>	Read-only	This option is used to override persistency when order is configured for

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			services or servicegroups. Default value: NO Possible values = YES, NO
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- UPDATE
- UNSET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbparameter **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"gslbparameter":{

"ldnsentrytimeout":<Integer_value>,

"rtttolerance":<Integer_value>,

"ldnsmask":<String_value>,

"v6ldnsmasklen":<Integer_value>,

"ldnsprobeorder":<String[]_value>,

"dropldnsreq":<String_value>,

"gslbsvcstatedelaytime":<Integer_value>,

"svcstatelearningtime":<Integer_value>,

"automaticconfigsync":<String_value>,

"mepkeepalivetimeout":<Integer_value>,

"gslbsyncinterval":<Integer_value>,

"gslbsyncmode":<String_value>,

"gslbsynclocfiles":<String_value>,

"gslbconfigsyncmonitor":<String_value>,
```

```
"gslbsyncsaveconfigcommand":<String_value>,

"undefaction":<String_value>,

"usekrpcchannelforsync":<String_value>,

"sourceipwhitelisting":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbparameter? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"gslbparameter":{

"ldnsentrytimeout":true,

"rtttolerance":true,

"ldnsmask":true,

"v6ldnsmasklen":true,

"ldnsprobeorder":true,

"dropldnsreq":true,
```

```
"gslbsvcstatedelaytime":true,

"svcstatelearningtime":true,

"automaticconfigsync":true,

"mepkeepalivetimeout":true,

"gslbsyncinterval":true,

"gslbsyncmode":true,

"gslbsynclocfiles":true,

"gslbconfigsyncmonitor":true,

"gslbsyncsaveconfigcommand":true,

"undefaction":true,

"usekrpcchannelforsync":true,

"sourceipwhitelisting":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbparameter **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "gslbparameter": [ {

"flags":<Integer_value>,

"ldnsentrytimeout":<Integer_value>,

"rtttolerance":<Integer_value>,

"ldnsmask":<String_value>,

"v6ldnsmasklen":<Integer_value>,

"ldnsprobeorder":<String[]_value>,

"dropldnsreq":<String_value>,

"gslbsvcstatedelaytime":<Integer_value>,

"svcstatelearningtime":<Integer_value>,

"automaticconfigsync":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"mepkeepalivetimeout":<Integer_value>,

"gslbsyncinterval":<Integer_value>,

"gslbsyncmode":<String_value>,

"incarnation":<Integer_value>,
```

```
"gslbsynclocfiles":<String_value>,

"gslbconfigsyncmonitor":<String_value>,

"gslbsyncsaveconfigcommand":<String_value>,

"undefaction":<String_value>,

"overridepersistencyfororder":<String_value>,

"usekrpcchannelforsync":<String_value>,

"sourceipwhitelisting":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

gslbrunningconfig

Configuration for running GSLB configuration resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
response	<String>	Read-only	gslb sync status as text blob.
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbrunningconfig

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "gslbrunningconfig": [ {

"response":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

gslbservice

Configuration for GSLB service resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
servicename	<String>	Read-write	Name for the GSLB service. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Can be changed after the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			GSLB service is created. CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my gslbsvc" or 'my gslbsvc'). Minimum length = 1
cnameentry	<String>	Read-write	Canonical name of the GSLB service. Used in CNAME-based GSLB. Minimum length = 1
ip	<String>	Read-write	IP address for the GSLB service. Should represent a load balancing, content switching, or VPN virtual server on the Citrix ADC, or the IP address of another load balancing device. Minimum length = 1
servername	<String>	Read-write	Name of the server hosting the GSLB service. Minimum length = 1
servicetype	<String>	Read-write	Type of service to create.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: NSSVC_SERVICE_UNKNOWN Possible values = HTTP, FTP, TCP, UDP, SSL, SSL_BRIDGE, SSL_TCP, NNTP, ANY, SIP_UDP, SIP_TCP, SIP_SSL, RADIUS, RDP, RTSP, MYSQL, MSSQL, ORACLE
port	<Integer>	Read-write	Port on which the load balancing entity represented by this GSLB service listens. Minimum value = 1 Range 1 - 65535 * in CLI is represented as 65535 in NITRO API
publicip	<String>	Read-write	The public IP address that a NAT device translates to the GSLB service's private IP address. Optional.
publicport	<Integer>	Read-write	The public port associated with the GSLB service's public IP address.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			The port is mapped to the service's private port number. Applicable to the local GSLB service. Optional.
maxclient	<Integer>	Read-write	The maximum number of open connections that the service can support at any given time. A GSLB service whose connection count reaches the maximum is not considered when a GSLB decision is made, until the connection count drops below the maximum. Minimum value = 0 Maximum value = 4294967294
healthmonitor	<String>	Read-write	Monitor the health of the GSLB service. Default value: YES Possible values = YES, NO
sitename	<String>	Read-write	Name of the GSLB site to which the service belongs. Minimum length = 1
state	<String>	Read-write	Enable or disable the service.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: ENABLED Possible values = ENABLED, DISABLED
cip	<String>	Read-write	In the request that is forwarded to the GSLB service, insert a header that stores the client's IP address. Client IP header insertion is used in connection-proxy based site persistence. Default value: DISABLED Possible values = ENABLED, DISABLED
cipheader	<String>	Read-write	Name for the HTTP header that stores the client's IP address. Used with the Client IP option. If client IP header insertion is enabled on the service and a name is not specified for the header, the Citrix ADC uses the name specified by the cipHeader parameter in the set ns param command or, in the GUI, the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Client IP Header parameter in the Configure HTTP Parameters dialog box. Minimum length = 1
sitepersistence	<String>	Read-write	Use cookie-based site persistence. Applicable only to HTTP and SSL GSLB services. Possible values = ConnectionProxy, HTTPRedirect, NONE
cookietimeout	<Integer>	Read-write	Timeout value, in minutes, for the cookie, when cookie based site persistence is enabled. Minimum value = 0 Maximum value = 1440
siteprefix	<String>	Read-write	The site's prefix string. When the service is bound to a GSLB virtual server, a GSLB site domain is generated internally for each bound service-domain pair by concatenating the site prefix of the service and the name of the domain.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			If the special string NONE is specified, the site-prefix string is unset. When implementing HTTP redirect site persistence, the Citrix ADC redirects GSLB requests to GSLB services by using their site domains.
clttimeout	<Integer>	Read-write	Idle time, in seconds, after which a client connection is terminated. Applicable if connection proxy based site persistence is used. Minimum value = 0 Maximum value = 31536000
svrtimeout	<Integer>	Read-write	Idle time, in seconds, after which a server connection is terminated. Applicable if connection proxy based site persistence is used. Minimum value = 0 Maximum value = 31536000
maxbandwidth	<Integer>	Read-write	Integer specifying the maximum

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			bandwidth allowed for the service. A GSLB service whose bandwidth reaches the maximum is not considered when a GSLB decision is made, until its bandwidth consumption drops below the maximum.
downstateflush	<String>	Read-write	Flush all active transactions associated with the GSLB service when its state transitions from UP to DOWN. Do not enable this option for services that must complete their transactions. Applicable if connection proxy based site persistence is used. Possible values = ENABLED, DISABLED
maxaaausers	<Integer>	Read-write	Maximum number of SSL VPN users that can be logged on concurrently to the VPN virtual server that is represented by this GSLB service. A GSLB service whose user count reaches the maximum is not

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			considered when a GSLB decision is made, until the count drops below the maximum. Minimum value = 0 Maximum value = 65535
monthreshold	<Integer>	Read-write	Monitoring threshold value for the GSLB service. If the sum of the weights of the monitors that are bound to this GSLB service and are in the UP state is not equal to or greater than this threshold value, the service is marked as DOWN. Minimum value = 0 Maximum value = 65535
hashid	<Integer>	Read-write	Unique hash identifier for the GSLB service, used by hash based load balancing methods. Minimum value = 1
comment	<String>	Read-write	Any comments that you might want to associate with the GSLB service.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
appflowlog	<String>	Read-write	Enable logging appflow flow information. Default value: ENABLED Possible values = ENABLED, DISABLED
naptrreplacement	<String>	Read-write	The replacement domain name for this NAPTR. Maximum length = 255
naptrorder	<Integer>	Read-write	An integer specifying the order in which the NAPTR records MUST be processed in order to accurately represent the ordered list of Rules. The ordering is from lowest to highest. Default value: 1 Minimum value = 1 Maximum value = 65535
naptrservices	<String>	Read-write	Service Parameters applicable to this delegation path. Maximum length = 255

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
naptrdomainttl	<Integer>	Read-write	Modify the TTL of the internally created naptr domain. Default value: 3600 Minimum value = 1
naptrpreference	<Integer>	Read-write	An integer specifying the preference of this NAPTR among NAPTR records having same order. lower the number, higher the preference. Default value: 1 Minimum value = 1 Maximum value = 65535
ipaddress	<String>	Read-write	The new IP address of the service.
viewname	<String>	Read-write	Name of the DNS view of the service. A DNS view is used in global server load balancing (GSLB) to return a predetermined IP address to a specific group of clients, which are identified by using a DNS policy. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
viewip	<String>	Read-write	IP address to be used for the given view.
weight	<Integer>	Read-write	Weight to assign to the monitor-service binding. A larger number specifies a greater weight. Contributes to the monitoring threshold, which determines the state of the service. Minimum value = 1 Maximum value = 100
monitor_name_svc	<String>	Read-write	Name of the monitor to bind to the service. Minimum length = 1
newname	<String>	Read-write	New name for the GSLB service. Minimum length = 1
gslb	<String>	Read-only	. Default value: GSLB Possible values = REMOTE, LOCAL
svrstate	<String>	Read-only	Server state. Possible values = UP, DOWN, UNKNOWN, BUSY, OUT OF SERVICE, GOING OUT OF

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			SERVICE, DOWN WHEN GOING OUT OF SERVICE, NS_EMPTY_STR, Unknown, DISABLED
svreffgslbstate	<String>	Read-only	Effective state of the gslb svc. Possible values = UP, DOWN, UNKNOWN, BUSY, OUT OF SERVICE, GOING OUT OF SERVICE, DOWN WHEN GOING OUT OF SERVICE, NS_EMPTY_STR, Unknown, DISABLED
gslbthreshold	<Integer>	Read-only	Indicates if gslb svc has reached threshold.
gslbsvcstats	<Integer>	Read-only	Indicates if gslb svc has stats of the primary or the whole chain.
monstate	<String>	Read-only	State of the monitor bound to gslb service. Possible values = ENABLED, DISABLED
preferredlocation	<String>	Read-only	Prefered location.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
monitor_state	<String>	Read-only	The running state of the monitor on this service. Possible values = UP, DOWN, UNKNOWN, BUSY, OUT OF SERVICE, GOING OUT OF SERVICE, DOWN WHEN GOING OUT OF SERVICE, NS_EMPTY_STR, Unknown, DISABLED
statechangetimesec	<String>	Read-only	Time when last state change happened. Seconds part.
tickssincelaststatechange	<Integer>	Read-only	Time in 10 millisecond ticks since the last state change.
threshold	<String>	Read-only	. Possible values = ABOVE, BELOW
clmonowner	<Integer>	Read-only	Tells the mon owner of the gslb service. Minimum value = 0 Maximum value = 32
clmonview	<Integer>	Read-only	Tells the view id of the monitoring owner.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
gslbsvchealth	<Integer>	Read-only	This parameter displays effective health of a GSLB service.
glsbsvchealthdescr	<String>	Read-only	Displays the warning message related to health a of GSLB service.
nodefaultbindings	<String>	Read-only	to determine if the configuration will have default ssl CIPHER and ECC curve bindings. Default value: NO Possible values = YES, NO
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT
- RENAME

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbservice **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"gslbservice":{

<b>"servicename":<String_value>,

</b>"cnameentry":<String_value>,

"ip":<String_value>,
```

```
"servername":<String_value>,

"servicetype":<String_value>,

"port":<Integer_value>,

"publicip":<String_value>,

"publicport":<Integer_value>,

"maxclient":<Integer_value>,

"healthmonitor":<String_value>,

<b>"sitename":<String_value>,

</b>"state":<String_value>,

"cip":<String_value>,

"cipheader":<String_value>,

"sitepersistence":<String_value>,

"cookietimeout":<Integer_value>,

"siteprefix":<String_value>,

"clttimeout":<Integer_value>,

"svrtimeout":<Integer_value>,

"maxbandwidth":<Integer_value>,

"downstateflush":<String_value>,

"maxaaausers":<Integer_value>,

"monthreshold":<Integer_value>,

"hashid":<Integer_value>,

"comment":<String_value>,
```

```
"appflowlog":<String_value>,

"naptrreplacement":<String_value>,

"naptrorder":<Integer_value>,

"naptrservices":<String_value>,

"naptrdomainttl":<Integer_value>,

"naptrpreference":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbservice/ servicename_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbservice **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"gslbservice":{

<b>"servicename":<String_value>,

</b>"ipaddress":<String_value>,

"publicip":<String_value>,

"publicport":<Integer_value>,

"cip":<String_value>,

"cipheader":<String_value>,

"sitepersistence":<String_value>,

"siteprefix":<String_value>,

"maxclient":<Integer_value>,

"healthmonitor":<String_value>,

"maxbandwidth":<Integer_value>,

"downstateflush":<String_value>,

"maxaaausers":<Integer_value>,

"viewname":<String_value>,

"viewip":<String_value>,

"monthreshold":<Integer_value>,

"weight":<Integer_value>,

"monitor_name_svc":<String_value>,

"hashid":<Integer_value>,

"comment":<String_value>,

"appflowlog":<String_value>,
```

```
"naptrorder":<Integer_value>,

"naptrpreference":<Integer_value>,

"naptrservices":<String_value>,

"naptrreplacement":<String_value>,

"naptrdomainttl":<Integer_value>,

"sitename":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbservice? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"gslbservice":{

<b>"servicename":<String_value>,

</b>"publicip":true,

"publicport":true,

"cip":true,
```

```
"cipheader":true,

"sitepersistence":true,

"siteprefix":true,

"maxclient":true,

"healthmonitor":true,

"maxbandwidth":true,

"downstateflush":true,

"maxaaausers":true,

"monthreshold":true,

"hashid":true,

"comment":true,

"appflowlog":true,

"naptrorder":true,

"naptrpreference":true,

"naptrservices":true,

"naptrreplacement":true,

"naptrdomainttl":true

}}
```


Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

RENAME

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbservice? **action=rename HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"gslbservice":{

<b>"servicename":<String_value>,

</b><b>"newname":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbservice **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/gslbservice? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/gslbservice? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of gslbservice resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/gslbservice? **view=summary**

Use this query-parameter to get the summary output of gslbservice resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/gslbservice? **pagesize=#no;pageno=#no**

Use this query-parameter to get the gslbservice resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "gslbservice": [ {

"servicename":<String_value>,

"gslb":<String_value>,

"ipaddress":<String_value>,

"ip":<String_value>,

"servername":<String_value>,

"servicetype":<String_value>,

"port":<Integer_value>,

"publicip":<String_value>,

"publicport":<Integer_value>,
```

```
"maxclient":<Integer_value>,

"maxaaausers":<Integer_value>,

"sitename":<String_value>,

"svrstate":<String_value>,

"svreffgslbstate":<String_value>,

"gslbthreshold":<Integer_value>,

"gslbsvcstats":<Integer_value>,

"state":<String_value>,

"monstate":<String_value>,

"cip":<String_value>,

"cipheader":<String_value>,

"sitepersistence":<String_value>,

"siteprefix":<String_value>,

"clttimeout":<Integer_value>,

"svrtimeout":<Integer_value>,

"preferredlocation":<String_value>,

"maxbandwidth":<Integer_value>,

"downstateflush":<String_value>,

"cnameentry":<String_value>,

"viewname":<String_value>,

"viewip":<String_value>,

"weight":<Integer_value>,
```

```
"monthreshold":<Integer_value>,

"monitor_state":<String_value>,

"hashid":<Integer_value>,

"comment":<String_value>,

"healthmonitor":<String_value>,

"appflowlog":<String_value>,

"statechangetimesec":<String_value>,

"tickssincelaststatechange":<Integer_value>,

"threshold":<String_value>,

"clmonowner":<Integer_value>,

"clmonview":<Integer_value>,

"naptrorder":<Integer_value>,

"naptrpreference":<Integer_value>,

"naptrservices":<String_value>,

"naptrreplacement":<String_value>,

"naptrdomainttl":<Integer_value>,

"gslbsvchealth":<Integer_value>,

"glsbsvchealthdescr":<String_value>,

"nodefaultbindings":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbservice/ servicename_value<String>
Query-parameters: attrs http:// <netscaler-ip-address> /nitro/v1/config/gslbservice/ servicename_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/gslbservice/ servicename_value<String> ? **view=summary**

Use this query-parameter to get the summary output of gslbservice resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "gslbservice": [ {

"servicename":<String_value>,

"gslb":<String_value>,

"ipaddress":<String_value>,
```

```
"ip":<String_value>,

"servername":<String_value>,

"servicetype":<String_value>,

"port":<Integer_value>,

"publicip":<String_value>,

"publicport":<Integer_value>,

"maxclient":<Integer_value>,

"maxaaausers":<Integer_value>,

"sitename":<String_value>,

"svrstate":<String_value>,

"svreffgslbstate":<String_value>,

"gslbthreshold":<Integer_value>,

"gslbsvcstats":<Integer_value>,

"state":<String_value>,

"monstate":<String_value>,

"cip":<String_value>,

"cipheader":<String_value>,

"sitepersistence":<String_value>,

"siteprefix":<String_value>,

"clttimeout":<Integer_value>,

"svrtimeout":<Integer_value>,

"preferredlocation":<String_value>,
```

```
"maxbandwidth":<Integer_value>,

"downstateflush":<String_value>,

"cnameentry":<String_value>,

"viewname":<String_value>,

"viewip":<String_value>,

"weight":<Integer_value>,

"monthreshold":<Integer_value>,

"monitor_state":<String_value>,

"hashid":<Integer_value>,

"comment":<String_value>,

"healthmonitor":<String_value>,

"appflowlog":<String_value>,

"statechangetimesec":<String_value>,

"tickssincelaststatechange":<Integer_value>,

"threshold":<String_value>,

"clmonowner":<Integer_value>,

"clmonview":<Integer_value>,

"naptrorder":<Integer_value>,

"naptrpreference":<Integer_value>,

"naptrservices":<String_value>,

"naptrreplacement":<String_value>,

"naptrdomainttl":<Integer_value>,
```

```
"gslbsvchealth":<Integer_value>,

"glsbsvchealthdescr":<String_value>,

"nodefaultbindings":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbservice? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "gslbservice": [ { "__count": "#no"} ] }
```

gslbservice_binding

Binding object which returns the resources bound to gslbservice.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
servicename	<String>	Read-write	Name of the GSLB service. Minimum length = 1
gslbservice_dnsview_binding	<gslbservice_dnsview_binding[]>	Read-only	dnsview that can be bound to gslbservice.
gslbservice_lbmonitor_binding	<gslbservice_lbmonitor_binding[]>	Read-only	lbmonitor that can be bound to gslbservice.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbservice_binding/ servicename_value<String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "gslbservice_binding": [ {

"servicename":<String_value>,

"gslbservice_dnsview_binding":<gslbservice_dnsview_binding[]_value>,

"gslbservice_lbmonitor_binding":<gslbservice_lbmonitor_binding[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbservice_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/gslbservice_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "gslbservice_binding": [ {

"servicename":<String_value>,

"gslbservice_dnsview_binding":<gslbservice_dnsview_binding[]_value>,

"gslbservice_lbmonitor_binding":<gslbservice_lbmonitor_binding[]_value>

}]}
```

gslbservice_dnsview_binding

Binding object showing the dnsview that can be bound to gslbservice.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
viewname	<String>	Read-write	Name of the DNS view of the service. A DNS view is used in global server load balancing (GSLB) to

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			return a predetermined IP address to a specific group of clients, which are identified by using a DNS policy. Minimum length = 1
servicename	<String>	Read-write	Name of the GSLB service. Minimum length = 1
viewip	<String>	Read-write	IP address to be used for the given view.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/gslbservice_dnsview_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"gslbservice_dnsview_binding":{

<b>"servicename":<String_value>,

</b>"viewname":<String_value>,

"viewip":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbservice_dnsview_binding/ servicename_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/ config/gslbservice_dnsview_binding/ servicename_value<String> ? **args=viewname: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbservice_dnsview_binding/ servicename_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/ config/gslbservice_dnsview_binding/ servicename_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of gslbservice_dnsview_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/gslbservice_dnsview_binding/ servicename_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the gslbservice_dnsview_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "gslbservice_dnsview_binding": [ {

"viewname":<String_value>,

"servicename":<String_value>,

"viewip":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbservice_dnsview_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/gslbservice_dnsview_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "gslbservice_dnsview_binding": [ {

"viewname":<String_value>,

"servicename":<String_value>,

"viewip":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbservice_dnsview_binding/ servicename_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"gslbservice_dnsview_binding": [ { "__count": "#no"} ] }
```

gslbservice_lbmonitor_binding

Binding object showing the lbmonitor that can be bound to gslbservice.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
monstate	<String>	Read-write	State of the monitor bound to gslb service. Possible values = ENABLED, DISABLED
weight	<Integer>	Read-write	Weight to assign to the monitor-service binding. A larger number specifies a greater weight. Contributes to the monitoring threshold, which determines the state of the service. Minimum value = 1 Maximum value = 100
servicename	<String>	Read-write	Name of the GSLB service. Minimum length = 1
monitor_name	<String>	Read-write	Monitor name.
totalfailedprobes	<Integer>	Read-only	The total number of failed probs.
monstatcode	<Integer>	Read-only	The code indicating the monitor response.
monitortotalprobes	<Integer>	Read-only	Total number of probes sent to monitor this service.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
monitortotalfailedprobes	<Integer>	Read-only	Total number of failed probes.
monstatparam2	<Integer>	Read-only	Second parameter for use with message code.
failedprobes	<Integer>	Read-only	Number of the current failed monitoring probes.
lastresponse	<String>	Read-only	Displays the gslb monitor status in string format.
responsetime	<Integer>	Read-only	Response time of this monitor.
monstatparam3	<Integer>	Read-only	Third parameter for use with message code.
monitor_state	<String>	Read-only	The running state of the monitor on this service. Possible values = UP, DOWN, UNKNOWN, BUSY, OUT OF SERVICE, GOING OUT OF SERVICE, DOWN WHEN GOING OUT OF SERVICE, NS_EMPTY_STR, Unknown, DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
monitorcurrentfailedprobes	<Integer>	Read-only	Total number of currently failed probes.
monstatparam1	<Integer>	Read-only	First parameter for use with message code.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/gslbservice_lbmonitor_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"gslbservice_lbmonitor_binding":{

<b>"servicename":<String_value>,

</b>"monitor_name":<String_value>,

"monstate":<String_value>,

"weight":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbservice_lbmonitor_binding/ servicename_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/

config/gslbservice_lbmonitor_binding/ servicename_value<String> ? **args=monitor_name: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbservice_lbmonitor_binding/ servicename_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/ config/gslbservice_lbmonitor_binding/ servicename_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of gslbservice_lbmonitor_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/gslbservice_lbmonitor_binding/ servicename_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the gslbservice_lbmonitor_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "gslbservice_lbmonitor_binding": [ {

"monstate":<String_value>,

"weight":<Integer_value>,

"servicename":<String_value>,

"monitor_name":<String_value>,

"totalfailedprobes":<Integer_value>,

"monstatcode":<Integer_value>,

"monitortotalprobes":<Integer_value>,

"monitortotalfailedprobes":<Integer_value>,

"monstatparam2":<Integer_value>,

"failedprobes":<Integer_value>,

"lastresponse":<String_value>,

"responsetime":<Integer_value>,

"monstatparam3":<Integer_value>,

"monitor_state":<String_value>,

"monitorcurrentfailedprobes":<Integer_value>,

"monstatparam1":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbservice_lbmonitor_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ gslbservice_lbmonitor_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "gslbservice_lbmonitor_binding": [ {

"monstate":<String_value>,

"weight":<Integer_value>,

"servicename":<String_value>,

"monitor_name":<String_value>,

"totalfailedprobes":<Integer_value>,

"monstatcode":<Integer_value>,

"monitortotalprobes":<Integer_value>,

"monitortotalfailedprobes":<Integer_value>,

"monstatparam2":<Integer_value>,
```

```
"failedprobes":<Integer_value>,

"lastresponse":<String_value>,

"responsetime":<Integer_value>,

"monstatparam3":<Integer_value>,

"monitor_state":<String_value>,

"monitorcurrentfailedprobes":<Integer_value>,

"monstatparam1":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbservice_lbmonitor_binding/servicename_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"gslbservice_lbmonitor_binding": [ { "__count": "#no"} ] }
```

gslbservicegroup

Configuration for GSLB service group resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
servicegroupname	<String>	Read-write	Name of the GSLB service group. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Can be changed after the name is created. Minimum length = 1
servicetype	<String>	Read-write	Protocol used to exchange data with the GSLB service. Possible values = HTTP, FTP, TCP, UDP, SSL, SSL_BRIDGE, SSL_TCP, NNTP, ANY, SIP_UDP, SIP_TCP, SIP_SSL, RADIUS, RDP, RTSP, MYSQL, MSSQL, ORACLE

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
maxclient	<Integer>	Read-write	Maximum number of simultaneous open connections for the GSLB service group. Minimum value = 0 Maximum value = 4294967294
cip	<String>	Read-write	Insert the Client IP header in requests forwarded to the GSLB service. Possible values = ENABLED, DISABLED
cipheader	<String>	Read-write	Name of the HTTP header whose value must be set to the IP address of the client. Used with the Client IP parameter. If client IP insertion is enabled, and the client IP header is not specified, the value of Client IP Header parameter or the value set by the set ns config command is used as client's IP header name. Minimum length = 1
healthmonitor	<String>	Read-write	Monitor the health of this GSLB service.Available

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			settings function are as follows: YES - Send probes to check the health of the GSLB service. NO - Do not send probes to check the health of the GSLB service. With the NO option, the appliance shows the service as UP at all times. Default value: YES Possible values = YES, NO
clttimeout	<Integer>	Read-write	Time, in seconds, after which to terminate an idle client connection. Minimum value = 0 Maximum value = 31536000
svrtimeout	<Integer>	Read-write	Time, in seconds, after which to terminate an idle server connection. Minimum value = 0 Maximum value = 31536000

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
maxbandwidth	<Integer>	Read-write	Maximum bandwidth, in Kbps, allocated for all the services in the GSLB service group. Minimum value = 0 Maximum value = 4294967287
monthreshold	<Integer>	Read-write	Minimum sum of weights of the monitors that are bound to this GSLB service. Used to determine whether to mark a GSLB service as UP or DOWN. Minimum value = 0 Maximum value = 65535
state	<String>	Read-write	Initial state of the GSLB service group. Default value: ENABLED Possible values = ENABLED, DISABLED
downstateflush	<String>	Read-write	Flush all active transactions associated with all the services in the GSLB service group whose state transitions from UP to DOWN. Do not enable this option for

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			applications that must complete their transactions. Default value: ENABLED Possible values = ENABLED, DISABLED
comment	<String>	Read-write	Any information about the GSLB service group.
appflowlog	<String>	Read-write	Enable logging of AppFlow information for the specified GSLB service group. Default value: ENABLED Possible values = ENABLED, DISABLED
autoscale	<String>	Read-write	Auto scale option for a GSLB servicegroup. Default value: DISABLED Possible values = DISABLED, DNS
autodelayedtrofs	<String>	Read-write	Indicates graceful movement of the service to TROFS. System will wait for monitor response

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			time out before moving to TROFS. Default value: NO Possible values = YES, NO
sitename	<String>	Read-write	Name of the GSLB site to which the service group belongs. Minimum length = 1
sitepersistence	<String>	Read-write	Use cookie-based site persistence. Applicable only to HTTP and SSL non-autoscale enabled GSLB servicegroups. Possible values = ConnectionProxy, HTTPRedirect, NONE
servername	<String>	Read-write	Name of the server to which to bind the service group. Minimum length = 1
port	<Integer>	Read-write	Server port number. Range 1 - 65535 * in CLI is represented as 65535 in NITRO API
weight	<Integer>	Read-write	Weight to assign to the servers in the service group.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Specifies the capacity of the servers relative to the other servers in the load balancing configuration. The higher the weight, the higher the percentage of requests sent to the service. Minimum value = 1 Maximum value = 100
hashid	<Integer>	Read-write	The hash identifier for the service. This must be unique for each service. This parameter is used by hash based load balancing methods. Minimum value = 1
publicip	<String>	Read-write	The public IP address that a NAT device translates to the GSLB service's private IP address. Optional. Minimum length = 1
publicport	<Integer>	Read-write	The public port associated with the GSLB service's public IP address. The port is mapped to the service's private port number. Applicable to the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			local GSLB service. Optional.
siteprefix	<String>	Read-write	The site's prefix string. When the GSLB service group is bound to a GSLB virtual server, a GSLB site domain is generated internally for each bound serviceitem-domain pair by concatenating the site prefix of the service item and the name of the domain. If the special string NONE is specified, the site-prefix string is unset. When implementing HTTP redirect site persistence, the Citrix ADC redirects GSLB requests to GSLB services by using their site domains.
order	<Integer>	Read-write	Order number to be assigned to the gslb servicegroup member. Minimum value = 1 Maximum value = 8192
monitor_name_svc	<String>	Read-write	Name of the monitor bound to the GSLB

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			service group. Used to assign a weight to the monitor. Minimum length = 1
dup_weight	<Integer>	Read-write	weight of the monitor that is bound to GSLB servicegroup. Minimum value = 1
delay	<Integer>	Read-write	The time allowed (in seconds) for a graceful shutdown. During this period, new connections or requests will continue to be sent to this service for clients who already have a persistent session on the system. Connections or requests from fresh or new clients who do not yet have a persistence sessions on the system will not be sent to the service. Instead, they will be load balanced among other available services. After the delay time expires, no new requests or connections will be sent to the service.
graceful	<String>	Read-write	Wait for all existing connections to the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			service to terminate before shutting down the service. Default value: NO Possible values = YES, NO
includemembers	<Boolean>	Read-write	Display the members of the listed GSLB service groups in addition to their settings. Can be specified when no service group name is provided in the command. In that case, the details displayed for each service group are identical to the details displayed when a service group name is provided, except that bound monitors are not displayed.
newname	<String>	Read-write	New name for the GSLB service group. Minimum length = 1
numofconnections	<Integer>	Read-only	This will tell the number of client side connections are still open.
serviceconftype	<Boolean>	Read-only	The configuration type of the GSLB service group.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
value	<String>	Read-only	SSL Status. Possible values = Certkey/ Certkeybundle/Vault not bound/Cert-store not usable, SSL feature disabled
svrstate	<String>	Read-only	The state of the GSLB service. Possible values = UP, DOWN, UNKNOWN, BUSY, OUT OF SERVICE, GOING OUT OF SERVICE, DOWN WHEN GOING OUT OF SERVICE, NS_EMPTY_STR, Unknown, DISABLED
ip	<String>	Read-only	IP Address.
monstatcode	<Integer>	Read-only	The code indicating the monitor response.
monstatparam1	<Integer>	Read-only	First parameter for use with message code.
monstatparam2	<Integer>	Read-only	Second parameter for use with message code.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
monstatparam3	<Integer>	Read-only	Third parameter for use with message code.
statechangetimemsec	<Integer>	Read-only	Time when last state change occurred. Milliseconds part.
stateupdatereason	<Integer>	Read-only	Checks state update reason on the secondary node.
clmonowner	<Integer>	Read-only	Tells the mon owner of the service.
clmonview	<Integer>	Read-only	Tells the view id of the monitoring owner.
groupcount	<Integer>	Read-only	Servicegroup Count.
serviceipstr	<String>	Read-only	This field has been intorduced to show the dbs services ip.
servicegroupeffectivestate	<String>	Read-only	Indicates the effective GSLB servicegroup state based on the state of the bound service items.If all services are UP the effective state is UP, if all are DOWN its DOWN,if all are OFS its OFS.If atleast one serviceis UP and rest are either DOWN or OFS, the effective state is PARTIAL-UP.If atleast one

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			bound service is DOWN and rest are OFS the effective state is PARTIAL DOWN. Possible values = UP, DOWN, OUT OF SERVICE, PARTIAL-UP, PARTIAL-DOWN
gslb	<String>	Read-only	. Default value: GSLB Possible values = REMOTE, LOCAL
svreffgslbstate	<String>	Read-only	Effective state of the gslb svc. Possible values = UP, DOWN, UNKNOWN, BUSY, OUT OF SERVICE, GOING OUT OF SERVICE, DOWN WHEN GOING OUT OF SERVICE, NS_EMPTY_STR, Unknown, DISABLED
nodefaultbindings	<String>	Read-only	to determine if the configuration is from stylebooks. Default value: NO

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = YES, NO
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- ENABLE
- DISABLE
- GET (ALL)
- GET
- COUNT
- RENAME

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbservicegroup **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"gslbservicegroup":{

<b>"servicegroupname":<String_value>,

</b><b>"servicetype":<String_value>,

</b>"maxclient":<Integer_value>,

"cip":<String_value>,

"cipheader":<String_value>,

"healthmonitor":<String_value>,

"clttimeout":<Integer_value>,

"svrtimeout":<Integer_value>,

"maxbandwidth":<Integer_value>,

"monthreshold":<Integer_value>,
```

```
"state":<String_value>,

"downstateflush":<String_value>,

"comment":<String_value>,

"appflowlog":<String_value>,

"autoscale":<String_value>,

"autodelayedtrofs":<String_value>,

<b>"sitename":<String_value>,

</b>"sitepersistence":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbservicegroup/ servicegroupname_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbservicegroup **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"gslbservicegroup":{

<b>"servicegroupname":<String_value>,

</b>"servername":<String_value>,

"port":<Integer_value>,

"weight":<Integer_value>,

"hashid":<Integer_value>,

"publicip":<String_value>,

"publicport":<Integer_value>,

"siteprefix":<String_value>,

"order":<Integer_value>,

"monitor_name_svc":<String_value>,

"dup_weight":<Integer_value>,

"maxclient":<Integer_value>,

"healthmonitor":<String_value>,

"cip":<String_value>,

"cipheader":<String_value>,

"clttimeout":<Integer_value>,

"svrtimeout":<Integer_value>,

"maxbandwidth":<Integer_value>,

"monthreshold":<Integer_value>,
```

```
"downstateflush":<String_value>,

"comment":<String_value>,

"appflowlog":<String_value>,

"sitepersistence":<String_value>,

"sitename":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbservicegroup? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"gslbservicegroup":{

<b>"servicegroupname":<String_value>,

</b>"servername":true,

"port":true,

"weight":true,

"hashid":true,
```

```
"publicip":true,

"publicport":true,

"siteprefix":true,

"order":true,

"maxclient":true,

"cip":true,

"clttimeout":true,

"svrtimeout":true,

"maxbandwidth":true,

"monthreshold":true,

"appflowlog":true,

"sitepersistence":true,

"monitor_name_svc":true,

"dup_weight":true,

"healthmonitor":true,

"cipheader":true,

"downstateflush":true,

"comment":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

ENABLE

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbservicegroup? **action=enable HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"gslbservicegroup":{

<b>"servicegroupname":<String_value>,

</b>"servername":<String_value>,

"port":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DISABLE

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbservicegroup? **action=disable HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"gslbservicegroup":{

<b>"servicegroupname":<String_value>,

</b>"servername":<String_value>,

"port":<Integer_value>,

"delay":<Integer_value>,

"graceful":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

RENAME

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbservicegroup? **action=rename HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"gslbservicegroup":{

<b>"servicegroupname":<String_value>,

</b><b>"newname":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbservicegroup **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/gslbservicegroup? **args=servicegroupname: <String_value> ,includemembers: <Boolean_value>**

Use this query-parameter to get gslbservicegroup resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/config/gslbservicegroup? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/gslbservicegroup? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of gslbservicegroup resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/gslbservicegroup? **view=summary**

Use this query-parameter to get the summary output of gslbservicegroup resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/gslbservicegroup? **pagesize=#no;pageno=#no**

Use this query-parameter to get the gslbservicegroup resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "gslbservicegroup": [ {

servicegroupname:<String_value>,includemembers:<Boolean_value>"numofconnec
tions":<Integer_value>,

"servicetype":<String_value>,

"port":<Integer_value>,

"serviceconftype":<Boolean_value>,

"value":<String_value>,

"maxclient":<Integer_value>,

"cip":<String_value>,

"cipheader":<String_value>,

"clttimeout":<Integer_value>,

"svrtimeout":<Integer_value>,

"maxbandwidth":<Integer_value>,

"state":<String_value>,

"svrstate":<String_value>,

"delay":<Integer_value>,

"ip":<String_value>,

"servername":<String_value>,

"monthreshold":<Integer_value>,
```

```
"weight":<Integer_value>,

"monstatcode":<Integer_value>,

"monstatparam1":<Integer_value>,

"monstatparam2":<Integer_value>,

"monstatparam3":<Integer_value>,

"downstateflush":<String_value>,

"statechangetimemsec":<Integer_value>,

"stateupdatereason":<Integer_value>,

"clmonowner":<Integer_value>,

"clmonview":<Integer_value>,

"groupcount":<Integer_value>,

"comment":<String_value>,

"hashid":<Integer_value>,

"graceful":<String_value>,

"healthmonitor":<String_value>,

"appflowlog":<String_value>,

"autoscale":<String_value>,

"autodelayedtrofs":<String_value>,

"serviceipstr":<String_value>,

"servicegroupeffectivestate":<String_value>,

"sitename":<String_value>,

"gslb":<String_value>,
```

```
"publicip":<String_value>,

"publicport":<Integer_value>,

"svreffgslbstate":<String_value>,

"sitepersistence":<String_value>,

"siteprefix":<String_value>,

"nodefaultbindings":<String_value>,

"order":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbservicegroup/ servicegroupname_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/gslbservicegroup/ servicegroupname_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/gslbservicegroup/ servicegroupname_value<String> ? **view=summary**

Use this query-parameter to get the summary output of gslbservicegroup resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "gslbservicegroup": [ {

servicegroupname:<String_value>,includemembers:<Boolean_value>"numofconnec
tions":<Integer_value>,

"servicetype":<String_value>,

"port":<Integer_value>,

"serviceconftype":<Boolean_value>,

"value":<String_value>,

"maxclient":<Integer_value>,

"cip":<String_value>,

"cipheader":<String_value>,

"clttimeout":<Integer_value>,

"svrtimeout":<Integer_value>,

"maxbandwidth":<Integer_value>,

"state":<String_value>,

"svrstate":<String_value>,

"delay":<Integer_value>,

"ip":<String_value>,
```

```
"servername":<String_value>,

"monthreshold":<Integer_value>,

"weight":<Integer_value>,

"monstatcode":<Integer_value>,

"monstatparam1":<Integer_value>,

"monstatparam2":<Integer_value>,

"monstatparam3":<Integer_value>,

"downstateflush":<String_value>,

"statechangetimemsec":<Integer_value>,

"stateupdatereason":<Integer_value>,

"clmonowner":<Integer_value>,

"clmonview":<Integer_value>,

"groupcount":<Integer_value>,

"comment":<String_value>,

"hashid":<Integer_value>,

"graceful":<String_value>,

"healthmonitor":<String_value>,

"appflowlog":<String_value>,

"autoscale":<String_value>,

"autodelayedtrofs":<String_value>,

"serviceipstr":<String_value>,

"servicegroupeffectivestate":<String_value>,
```

```
"sitename":<String_value>,

"gslb":<String_value>,

"publicip":<String_value>,

"publicport":<Integer_value>,

"svreffgslbstate":<String_value>,

"sitepersistence":<String_value>,

"siteprefix":<String_value>,

"nodefaultbindings":<String_value>,

"order":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbservicegroup? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "gslbservicegroup": [ { "__count": "#no"} ] }
```

gslbservicegroup_binding

Binding object which returns the resources bound to gslbservicegroup.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
servicegroupname	<String>	Read-write	Name of the GSLB service group. Minimum length = 1
gslbservicegroup_gslbservicegroupmember_binding	<gslbservicegroup_gslbservicegroupmember_binding[]>	Read-only	gslbservicegroupmember that can be bound to gslbservicegroup.
gslbservicegroup_servicegroupentitymonbindings_binding	<gslbservicegroup_servicegroupentitymonbindings_binding[]>	Read-only	servicegroupentitymonbindings that can be bound to gslbservicegroup.
gslbservicegroup_lbmonitor_binding	<gslbservicegroup_lbmonitor_binding[]>	Read-only	lbmonitor that can be bound to gslbservicegroup.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbservicegroup_binding/servicegroupname_value<String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "gslbservicegroup_binding": [ {

"servicegroupname":<String_value>,

"gslbservicegroup_gslbservicegroupmember_binding":<gslbservicegroup_gslbse
rvicegroupmember_binding[]_value>,

"gslbservicegroup_lbmonitor_binding":<gslbservicegroup_lbmonitor_binding[]
_value>,

"gslbservicegroup_servicegroupentitymonbindings_binding":<gslbservicegroup
_servicegroupentitymonbindings_binding[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbservicegroup_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/gslbservicegroup_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "gslbservicegroup_binding": [ {

"servicegroupname":<String_value>,

"gslbservicegroup_gslbservicegroupmember_binding":<gslbservicegroup_gslbse
rvicegroupmember_binding[]_value>,

"gslbservicegroup_lbmonitor_binding":<gslbservicegroup_lbmonitor_binding[]
_value>,

"gslbservicegroup_servicegroupentitymonbindings_binding":<gslbservicegroup
_servicegroupentitymonbindings_binding[]_value>

}]}
```

gslbservicegroup_gslbservicegroupmember_binding

Binding object showing the gslbservicegroupmember that can be bound to gslbservicegroup.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
servername	<String>	Read-write	Name of the server to which to bind the service group. Minimum length = 1
weight	<Integer>	Read-write	Weight to assign to the servers in the service group. Specifies the capacity of the servers relative to the other servers in the load balancing configuration. The higher the weight, the higher the percentage of

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			requests sent to the service. Minimum value = 1 Maximum value = 100
servicegroupname	<String>	Read-write	Name of the GSLB service group. Minimum length = 1
state	<String>	Read-write	Initial state of the GSLB service group. Default value: ENABLED Possible values = ENABLED, DISABLED
hashid	<Integer>	Read-write	The hash identifier for the service. This must be unique for each service. This parameter is used by hash based load balancing methods. Minimum value = 1
port	<Integer>	Read-write	Server port number. Range 1 - 65535 * in CLI is represented as 65535 in NITRO API
publicport	<Integer>	Read-write	The public port associated with the GSLB service's

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			public IP address. The port is mapped to the service's private port number. Applicable to the local GSLB service. Optional.
order	<Integer>	Read-write	Order number to be assigned to the gslb servicegroup member. Minimum value = 1 Maximum value = 8192
ip	<String>	Read-write	IP Address.
publicip	<String>	Read-write	The public IP address that a NAT device translates to the GSLB service's private IP address. Optional. Minimum length = 1
siteprefix	<String>	Read-write	The site's prefix string. When the GSLB service group is bound to a GSLB virtual server, a GSLB site domain is generated internally for each bound serviceitem-domain pair by concatenating the site prefix of the service item and the name of the domain.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			If the special string NONE is specified, the site-prefix string is unset. When implementing HTTP redirect site persistence, the Citrix ADC redirects GSLB requests to GSLB services by using their site domains.
statechangetimesec	<String>	Read-only	Time when last state change occurred. Seconds part.
delay	<Integer>	Read-only	The time allowed (in seconds) for a graceful shutdown. During this period, new connections or requests will continue to be sent to this service for clients who already have a persistent session on the system. Connections or requests from fresh or new clients who do not yet have a persistence sessions on the system will not be sent to the service. Instead, they will be load balanced among other available services. After the delay time

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			expires, no new requests or connections will be sent to the service.
gslbthreshold	<Integer>	Read-only	Indicates if gslb svc has reached threshold.
tickssincelaststatechange	<Integer>	Read-only	Time in 10 millisecond ticks since the last state change.
orderstr	<String>	Read-only	Order number in string form assigned to the gslb servicegroup member.
trofsdelay	<Integer>	Read-only	Delay before moving to TROFS.
svrstate	<String>	Read-only	The state of the GSLB service. Possible values = UP, DOWN, UNKNOWN, BUSY, OUT OF SERVICE, GOING OUT OF SERVICE, DOWN WHEN GOING OUT OF SERVICE, NS_EMPTY_STR, Unknown, DISABLED
threshold	<String>	Read-only	.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ABOVE, BELOW
preferredlocation	<String>	Read-only	Prefered location.
graceful	<String>	Read-only	Wait for all existing connections to the service to terminate before shutting down the service. Default value: NO Possible values = YES, NO
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of

creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/ gslbservicegroup_gslbservicegroupmember_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"gslbservicegroup_gslbservicegroupmember_binding":{

<b>"servicegroupname":<String_value>,

</b>"ip":<String_value>,

"servername":<String_value>,

"port":<Integer_value>,

"weight":<Integer_value>,

"state":<String_value>,
```

```
"hashid":<Integer_value>,

"publicip":<String_value>,

"publicport":<Integer_value>,

"siteprefix":<String_value>,

"order":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/ gslbservicegroup_gslbservicegroupmember_binding/ servicegroupname_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ gslbservicegroup_gslbservicegroupmember_binding/ servicegroupname_value<String> ? **args=ip: <String_value> ,servername: <String_value> ,port: <Integer_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/ gslbservicegroup_gslbservicegroupmember_binding/ servicegroupname_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/

gslbservicegroup_gslbservicegroupmember_binding/ servicegroupname_value<String> ?
filter=property-name1:property-value1,property-name2:property-value2

Use this query-parameter to get the filtered set of gslbservicegroup_gslbservicegroupmember_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ gslbservicegroup_gslbservicegroupmember_binding/ servicegroupname_value<String> ?
pagesize=#no;pageno=#no

Use this query-parameter to get the gslbservicegroup_gslbservicegroupmember_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "gslbservicegroup_gslbservicegroupmember_binding": [ {

"servername":<String_value>,

"weight":<Integer_value>,

"servicegroupname":<String_value>,

"state":<String_value>,

"hashid":<Integer_value>,
```

```
"port":<Integer_value>,

"publicport":<Integer_value>,

"order":<Integer_value>,

"ip":<String_value>,

"publicip":<String_value>,

"siteprefix":<String_value>,

"statechangetimesec":<String_value>,

"delay":<Integer_value>,

"gslbthreshold":<Integer_value>,

"tickssincelaststatechange":<Integer_value>,

"orderstr":<String_value>,

"trofsdelay":<Integer_value>,

"svrstate":<String_value>,

"threshold":<String_value>,

"preferredlocation":<String_value>,

"graceful":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/ gslbservicegroup_gslbservicegroupmember_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ gslbservicegroup_gslbservicegroupmember_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "gslbservicegroup_gslbservicegroupmember_binding": [ {

"servername":<String_value>,

"weight":<Integer_value>,

"servicegroupname":<String_value>,

"state":<String_value>,

"hashid":<Integer_value>,

"port":<Integer_value>,

"publicport":<Integer_value>,

"order":<Integer_value>,

"ip":<String_value>,

"publicip":<String_value>,

"siteprefix":<String_value>,
```

```
"statechangetimesec":<String_value>,

"delay":<Integer_value>,

"gslbthreshold":<Integer_value>,

"tickssincelaststatechange":<Integer_value>,

"orderstr":<String_value>,

"trofsdelay":<Integer_value>,

"svrstate":<String_value>,

"threshold":<String_value>,

"preferredlocation":<String_value>,

"graceful":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/ gslbservicegroup_gslbservicegroupmember_binding/ servicegroupname_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"gslbservicegroup_gslbservicegroupmember_binding": [ { "__count":
"#no"} ] }
```

gslbservicegroup_lbmonitor_binding

Binding object showing the lbmonitor that can be bound to gslbservicegroup.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
siteprefix	<String>	Read-write	The site's prefix string. When the GSLB service group is bound to a GSLB virtual server, a GSLB site domain is generated internally for each bound serviceitem-domain pair by concatenating the site prefix of the service item and the name of the domain. If the special string NONE is specified, the site-prefix string is unset. When implementing HTTP redirect site persistence, the Citrix ADC redirects GSLB requests to GSLB services by using their site domains.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
monitor_name	<String>	Read-write	Monitor name.
publicip	<String>	Read-write	The public IP address that a NAT device translates to the GSLB service's private IP address. Optional.
monstate	<String>	Read-write	Monitor state. Possible values = ENABLED, DISABLED
state	<String>	Read-write	Initial state of the service after binding. Default value: ENABLED Possible values = ENABLED, DISABLED
weight	<Integer>	Read-write	Weight to assign to the servers in the service group. Specifies the capacity of the servers relative to the other servers in the load balancing configuration. The higher the weight, the higher the percentage of requests sent to the service. Minimum value = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum value = 100
servicegroupname	<String>	Read-write	Name of the GSLB service group. Minimum length = 1
port	<Integer>	Read-write	Port number of the GSLB service. Each service must have a unique port number. Range 1 - 65535 * in CLI is represented as 65535 in NITRO API
publicport	<Integer>	Read-write	The public port associated with the GSLB service's public IP address. The port is mapped to the service's private port number. Applicable to the local GSLB service. Optional.
order	<Integer>	Read-write	Order number to be assigned to the gslb servicegroup member.
passive	<Boolean>	Read-write	Indicates if load monitor is passive. A passive load monitor does not remove service from LB decision when

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			threshold is breached.
hashid	<Integer>	Read-write	Unique numerical identifier used by hash based load balancing methods to identify a service. Minimum value = 1
monweight	<Integer>	Read-only	weight of the monitor that is bound to GSLB servicegroup.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of

creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/gslbservicegroup_lbmonitor_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"gslbservicegroup_lbmonitor_binding":{

<b>"servicegroupname":<String_value>,

</b>"port":<Integer_value>,

"monitor_name":<String_value>,

"monstate":<String_value>,

"passive":<Boolean_value>,

"weight":<Integer_value>,
```

```
"state":<String_value>,

"hashid":<Integer_value>,

"publicip":<String_value>,

"publicport":<Integer_value>,

"siteprefix":<String_value>,

"order":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbservicegroup_lbmonitor_binding/ servicegroupname_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/gslbservicegroup_lbmonitor_binding/ servicegroupname_value<String> ? **args=port: <Integer_value> ,monitor_name: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbservicegroup_lbmonitor_binding/ servicegroupname_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/

v1/config/gslbservicegroup_lbmonitor_binding/ servicegroupname_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of gslbservicegroup_lbmonitor_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/gslbservicegroup_lbmonitor_binding/ servicegroupname_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the gslbservicegroup_lbmonitor_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "gslbservicegroup_lbmonitor_binding": [ {

"siteprefix":<String_value>,

"monitor_name":<String_value>,

"publicip":<String_value>,

"monstate":<String_value>,

"state":<String_value>,

"weight":<Integer_value>,
```

```
"servicegroupname":<String_value>,

"port":<Integer_value>,

"publicport":<Integer_value>,

"order":<Integer_value>,

"passive":<Boolean_value>,

"hashid":<Integer_value>,

"monweight":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbservicegroup_lbmonitor_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/gslbservicegroup_lbmonitor_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "gslbservicegroup_lbmonitor_binding": [ {

"siteprefix":<String_value>,

"monitor_name":<String_value>,

"publicip":<String_value>,

"monstate":<String_value>,

"state":<String_value>,

"weight":<Integer_value>,

"servicegroupname":<String_value>,

"port":<Integer_value>,

"publicport":<Integer_value>,

"order":<Integer_value>,

"passive":<Boolean_value>,

"hashid":<Integer_value>,

"monweight":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbservicegroup_lbmonitor_binding/ servicegroupname_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"gslbservicegroup_lbmonitor_binding": [ { "__count": "#no"} ] }
```

gslbservicegroup_servicegroupentitymonbindings_binding

Binding object showing the servicegroupentitymonbindings that can be bound to gslbservicegroup.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
weight	<Integer>	Read-write	When used along with monitor name, it specifies the weight of the monitor binding. When used along with servername ; port pair, it specifies the weight of this GSLB service . Default value: 1 Minimum value = 1 Maximum value = 100
servicegroupname	<String>	Read-write	Name of the GSLB service group.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum length = 1
state	<String>	Read-write	Initial state of the service after binding. Default value: ENABLED Possible values = ENABLED, DISABLED
passive	<Boolean>	Read-write	Indicates if load monitor is passive. A passive load monitor does not remove service from LB decision when threshold is breached.
hashid	<Integer>	Read-write	Unique numerical identifier used by hash based load balancing methods to identify a service. Minimum value = 1
port	<Integer>	Read-write	Port number of the GSLB service. Each service must have a unique port number. Range 1 - 65535 * in CLI is represented as 65535 in NITRO API
publicport	<Integer>	Read-write	The public port associated with the GSLB service's

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			public IP address. The port is mapped to the service's private port number. Applicable to the local GSLB service. Optional.
order	<Integer>	Read-write	Order number to be assigned to the gslb servicegroup member.
publicip	<String>	Read-write	The public IP address that a NAT device translates to the GSLB service's private IP address. Optional.
siteprefix	<String>	Read-write	The site's prefix string. When the GSLB service group is bound to a GSLB virtual server, a GSLB site domain is generated internally for each bound serviceitem-domain pair by concatenating the site prefix of the service item and the name of the domain. If the special string NONE is specified, the site-prefix string is unset. When implementing HTTP redirect site persistence, the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Citrix ADC redirects GSLB requests to GSLB services by using their site domains.
monitor_name	<String>	Read-write	Monitor name.
servicegroupentname2	<String>	Read-write	.
monitorcurrentfailedprobes	<Integer>	Read-only	Total number of currently failed probes.
monitor_state	<String>	Read-only	The running state of the monitor on this service. Possible values = UP, DOWN, UNKNOWN, BUSY, OUT OF SERVICE, GOING OUT OF SERVICE, DOWN WHEN GOING OUT OF SERVICE, NS_EMPTY_STR, Unknown, DISABLED
lastresponse	<String>	Read-only	The string form of monstatcode.
monitortotalfailedprobes	<Integer>	Read-only	Total number of failed probes.
monitortotalprobes	<Integer>	Read-only	Total number of probes sent to monitor this service.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/ gslbservicegroup_servicegroupentitymonbindings_binding/ servicegroupname_value<String>
Query-parameters: filter http:// <netscaler-ip-address> /nitro/v1/config/ gslbservicegroup_servicegroupentitymonbindings_binding/ servicegroupname_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of gslbservicegroup_servicegroupentitymonbindings_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ gslbservicegroup_servicegroupentitymonbindings_binding/ servicegroupname_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the gslbservicegroup_servicegroupentitymonbindings_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "gslbservicegroup_servicegroupentitymonbindings_binding": [ {

"weight":<Integer_value>,

"servicegroupname":<String_value>,
```

```
"state":<String_value>,

"passive":<Boolean_value>,

"hashid":<Integer_value>,

"port":<Integer_value>,

"publicport":<Integer_value>,

"order":<Integer_value>,

"publicip":<String_value>,

"siteprefix":<String_value>,

"monitor_name":<String_value>,

"servicegroupentname2":<String_value>,

"monitorcurrentfailedprobes":<Integer_value>,

"monitor_state":<String_value>,

"lastresponse":<String_value>,

"monitortotalfailedprobes":<Integer_value>,

"monitortotalprobes":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/ gslbservicegroup_servicegroupentitymonbindings_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ gslbservicegroup_servicegroupentitymonbindings_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "gslbservicegroup_servicegroupentitymonbindings_binding": [ {

"weight":<Integer_value>,

"servicegroupname":<String_value>,

"state":<String_value>,

"passive":<Boolean_value>,

"hashid":<Integer_value>,

"port":<Integer_value>,

"publicport":<Integer_value>,

"order":<Integer_value>,

"publicip":<String_value>,

"siteprefix":<String_value>,

"monitor_name":<String_value>,

"servicegroupentname2":<String_value>,
```

```
"monitorcurrentfailedprobes":<Integer_value>,

"monitor_state":<String_value>,

"lastresponse":<String_value>,

"monitortotalfailedprobes":<Integer_value>,

"monitortotalprobes":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/ gslbservicegroup_servicegroupentitymonbindings_binding/ servicegroupname_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"gslbservicegroup_servicegroupentitymonbindings_binding": [ { "__count":
"#no"} ] }
```

gslbsite

Configuration for GSLB site resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
sitename	<String>	Read-write	Name for the GSLB site. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the virtual server is created. CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my gslbsite" or 'my gslbsite'). Minimum length = 1
sitetype	<String>	Read-write	Type of site to create. If the type is not specified, the appliance automatically detects and sets the type on the basis of the IP

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			address being assigned to the site. If the specified site IP address is owned by the appliance (for example, a MIP address or SNIP address), the site is a local site. Otherwise, it is a remote site. Default value: NONE Possible values = REMOTE, LOCAL
siteipaddress	<String>	Read-write	IP address for the GSLB site. The GSLB site uses this IP address to communicate with other GSLB sites. For a local site, use any IP address that is owned by the appliance (for example, a SNIP or MIP address, or the IP address of the ADNS service). Minimum length = 1
publicip	<String>	Read-write	Public IP address for the local site. Required only if the appliance is deployed in a private address space and the site has a public IP address hosted on

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			an external firewall or a NAT device. Minimum length = 1
metricexchange	<String>	Read-write	Exchange metrics with other sites. Metrics are exchanged by using Metric Exchange Protocol (MEP). The appliances in the GSLB setup exchange health information once every second. If you disable metrics exchange, you can use only static load balancing methods (such as round robin, static proximity, or the hash-based methods), and if you disable metrics exchange when a dynamic load balancing method (such as least connection) is in operation, the appliance falls back to round robin. Also, if you disable metrics exchange, you must use a monitor to

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			determine the state of GSLB services. Otherwise, the service is marked as DOWN. Default value: ENABLED Possible values = ENABLED, DISABLED
nwmetricexchange	<String>	Read-write	Exchange, with other GSLB sites, network metrics such as round-trip time (RTT), learned from communications with various local DNS (LDNS) servers used by clients. RTT information is used in the dynamic RTT load balancing method, and is exchanged every 5 seconds. Default value: ENABLED Possible values = ENABLED, DISABLED
sessionexchange	<String>	Read-write	Exchange persistent session entries with other GSLB sites every five seconds.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: ENABLED Possible values = ENABLED, DISABLED
triggermonitor	<String>	Read-write	Specify the conditions under which the GSLB service must be monitored by a monitor, if one is bound. Available settings function as follows: * ALWAYS - Monitor the GSLB service at all times. * MEPDOWN - Monitor the GSLB service only when the exchange of metrics through the Metrics Exchange Protocol (MEP) is disabled. MEPDOWN_SVCDOWN - Monitor the service in either of the following situations: * The exchange of metrics through MEP is disabled.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			* The exchange of metrics through MEP is enabled but the status of the service, learned through metrics exchange, is DOWN. Default value: ALWAYS Possible values = ALWAYS, MEPDOWN, MEPDOWN_SVCDOWN
parentsite	<String>	Read-write	Parent site of the GSLB site, in a parent-child topology.
clip	<String>	Read-write	Cluster IP address. Specify this parameter to connect to the remote cluster site for GSLB auto-sync. Note: The cluster IP address is defined when creating the cluster.
publicclip	<String>	Read-write	IP address to be used to globally access the remote cluster when it is deployed behind a NAT. It can be same

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			as the normal cluster IP address.
naptrreplacementsuffix	<String>	Read-write	The naptr replacement suffix configured here will be used to construct the naptr replacement field in NAPTR record. Minimum length = 1
backupparentlist	<String[]>	Read-write	The list of backup gslb sites configured in preferred order. Need to be parent gsb sites. Default value: "None"
sitepassword	<String>	Read-write	Password to be used for mep communication between gslb site nodes.
krpcnodesrcip	<String>	Read-write	Source IP address to be used to communicate with this GSLB site. Minimum length = 1
newname	<String>	Read-write	New name for the GSLB site. Minimum length = 1 Maximum length = 31
status	<String>	Read-only	Current metric exchange status.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ACTIVE, INACTIVE, DOWN
persistencemepstatus	<String>	Read-only	Network metric and persistence exchange MEP connection status. Possible values = ACTIVE, INACTIVE, DOWN
version	<Integer>	Read-only	will be true if the remote site's version is ncore compatible with the local site.(>= 9.2).
curbackupparentip	<String>	Read-only	Current active backup parent IP address since the configured is DOWN.
sitestate	<String>	Read-only	Site state. Possible values = UP, DOWN, UNKNOWN, BUSY, OUT OF SERVICE, GOING OUT OF SERVICE, DOWN WHEN GOING OUT OF SERVICE, NS_EMPTY_STR, Unknown, DISABLED
oldname	<String>	Read-only	Old name for the GSLB site. Must begin with an ASCII

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the virtual server is created. CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my gslbsite" or 'my gslbsite'). Minimum length = 1
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)

- GET
- COUNT
- RENAME

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbsite **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"gslbsite":{

<b>"sitename":<String_value>,

</b>"sitetype":<String_value>,

<b>"siteipaddress":<String_value>,

</b>"publicip":<String_value>,

"metricexchange":<String_value>,

"nwmetricexchange":<String_value>,

"sessionexchange":<String_value>,

"triggermonitor":<String_value>,

"parentsite":<String_value>,

"clip":<String_value>,

"publicclip":<String_value>,

"naptrreplacementsuffix":<String_value>,

"backupparentlist":<String[]_value>,

"sitepassword":<String_value>,

"krpcnodesrcip":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbsite/ sitename_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbsite **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"gslbsite":{

<b>"sitename":<String_value>,

</b>"metricexchange":<String_value>,

"nwmetricexchange":<String_value>,

"sessionexchange":<String_value>,

"triggermonitor":<String_value>,

"naptrreplacementsuffix":<String_value>,

"parentsite":<String_value>,

"backupparentlist":<String[]_value>,

"siteipaddress":<String_value>,
```

```
"publicip":<String_value>,

"krpcnodesrcip":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbsite? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"gslbsite":{

<b>"sitename":<String_value>,

</b>"metricexchange":true,

"nwmetricexchange":true,

"sessionexchange":true,

"triggermonitor":true,

"naptrreplacementsuffix":true,

"backupparentlist":true,

"krpcnodesrcip":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

RENAME

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbsite? **action=rename HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"gslbsite":{

<b>"sitename":<String_value>,

</b><b>"newname":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbsite **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/gslbsite? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/gslbsite? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of gslbsite resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/gslbsite? **view=summary**

Use this query-parameter to get the summary output of gslbsite resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/gslbsite? **pagesize=#no;pageno=#no**

Use this query-parameter to get the gslbsite resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "gslbsite": [ {

"sitename":<String_value>,

"sitetype":<String_value>,

"siteipaddress":<String_value>,

"publicip":<String_value>,

"metricexchange":<String_value>,
```

```
"status":<String_value>,

"persistencemepstatus":<String_value>,

"nwmetricexchange":<String_value>,

"sessionexchange":<String_value>,

"triggermonitor":<String_value>,

"parentsite":<String_value>,

"version":<Integer_value>,

"clip":<String_value>,

"publicclip":<String_value>,

"naptrreplacementsuffix":<String_value>,

"backupparentlist":<String[]_value>,

"curbackupparentip":<String_value>,

"sitestate":<String_value>,

"oldname":<String_value>,

"krpcnodesrcip":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbsite/ sitename_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/gslbsite/ sitename_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/gslbsite/ sitename_value<String> ? **view=summary**

Use this query-parameter to get the summary output of gslbsite resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "gslbsite": [ {

"sitename":<String_value>,

"sitetype":<String_value>,

"siteipaddress":<String_value>,

"publicip":<String_value>,

"metricexchange":<String_value>,

"status":<String_value>,

"persistencemepstatus":<String_value>,

"nwmetricexchange":<String_value>,
```

```
"sessionexchange":<String_value>,

"triggermonitor":<String_value>,

"parentsite":<String_value>,

"version":<Integer_value>,

"clip":<String_value>,

"publicclip":<String_value>,

"naptrreplacementsuffix":<String_value>,

"backupparentlist":<String[]_value>,

"curbackupparentip":<String_value>,

"sitestate":<String_value>,

"oldname":<String_value>,

"krpcnodesrcip":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbsite? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "gslbsite": [ { "__count": "#no"} ] }
```

gslbsite_binding

Binding object which returns the resources bound to gslbsite.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
sitename	<String>	Read-write	Name of the GSLB site. If you specify a site name, details of all the site's constituent services are also displayed. Minimum length = 1
gslbsite_gslbservice_binding	<gslbsite_gslbservice_binding[]>	Read-only	gslbservice that can be bound to gslbsite.
gslbsite_gslbservicegroupmember_binding	<gslbsite_gslbservicegroupmember_binding[]>	Read-only	gslbservicegroupmember that can be bound to gslbsite.
gslbsite_gslbservicegroup_binding	<gslbsite_gslbservicegroup_binding[]>	Read-only	gslbservicegroup that can be bound to gslbsite.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbsite_binding/ sitename_value<String>
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "gslbsite_binding": [ {

"sitename":<String_value>,

"gslbsite_gslbservicegroup_binding":<gslbsite_gslbservicegroup_binding[]_value>,

"gslbsite_gslbservice_binding":<gslbsite_gslbservice_binding[]_value>,

"gslbsite_gslbservicegroupmember_binding":<gslbsite_gslbservicegroupmember_binding[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbsite_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/gslbsite_binding?**bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "gslbsite_binding": [ {

"sitename":<String_value>,

"gslbsite_gslbservicegroup_binding":<gslbsite_gslbservicegroup_binding[]_value>,

"gslbsite_gslbservice_binding":<gslbsite_gslbservice_binding[]_value>,

"gslbsite_gslbservicegroupmember_binding":<gslbsite_gslbservicegroupmember_binding[]_value>

}]}
```

gslbsite_gslbservice_binding

Binding object showing the gslbservice that can be bound to gslbsite.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
sitename	<String>	Read-write	Name of the GSLB site. If you specify a site name, details of all the site's constituent services are also displayed. Minimum length = 1
servicename	<String>	Read-write	Service name.
ipaddress	<String>	Read-only	IP Address of the gslb service.
port	<Integer>	Read-only	Port number of the gslb service.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Range 1 - 65535 * in CLI is represented as 65535 in NITRO API
servicetype	<String>	Read-only	Service type. Possible values = HTTP, FTP, TCP, UDP, SSL, SSL_BRIDGE, SSL_TCP, DTLS, NNTP, DNS, DHCPRA, ANY, SIP_UDP, SIP_TCP, SIP_SSL, DNS_TCP, RTSP, PUSH, SSL_PUSH, RADIUS, RDP, MYSQL, MSSQL, DIAMETER, SSL_DIAMETER, TFTP, ORACLE, SMPP, SYSLOGTCP, SYSLOGUDP, FIX, SSL_FIX, PROXY, USER_TCP, USER_SSL_TCP, QUIC, IPFIX, LOGSTREAM, MONGO, MONGO_TLS, MQTT, MQTT_TLS, QUIC_BRIDGE, HTTP_QUIC, DOT,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			SSL_PROXY, KAFKA_PRODUCER
cnameentry	<String>	Read-only	The cname of the gslb service. Minimum length = 1
state	<String>	Read-only	State of the gslb service. Possible values = UP, DOWN, UNKNOWN, BUSY, OUT OF SERVICE, GOING OUT OF SERVICE, DOWN WHEN GOING OUT OF SERVICE, NS_EMPTY_STR, Unknown, DISABLED
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbsite_gslbservice_binding/ sitename_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ gslbsite_gslbservice_binding/ sitename_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of gslbsite_gslbservice_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/gslbsite_gslbservice_binding/ sitename_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the gslbsite_gslbservice_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "gslbsite_gslbservice_binding": [ {

"sitename":<String_value>,

"servicename":<String_value>,

"ipaddress":<String_value>,

"port":<Integer_value>,

"servicetype":<String_value>,

"cnameentry":<String_value>,

"state":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbsite_gslbservice_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/gslbsite_gslbservice_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "gslbsite_gslbservice_binding": [ {

"sitename":<String_value>,

"servicename":<String_value>,

"ipaddress":<String_value>,

"port":<Integer_value>,

"servicetype":<String_value>,

"cnameentry":<String_value>,

"state":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbsite_gslbservice_binding/ sitename_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"gslbsite_gslbservice_binding": [ { "__count": "#no"} ] }
```

gslbsite_gslbservicegroup_binding

Binding object showing the gslbservicegroup that can be bound to gslbsite.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
sitename	<String>	Read-write	Name of the GSLB site. If you specify a site name, details of all the site's constituent services are also displayed. Minimum length = 1
servicegroupname	<String>	Read-write	Servicegroup name.
servicetype	<String>	Read-only	Service type. Possible values = HTTP, FTP, TCP, UDP, SSL, SSL_BRIDGE, SSL_TCP, DTLS, NNTP, DNS, DHCPRA, ANY, SIP_UDP, SIP_TCP, SIP_SSL,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			DNS_TCP, RTSP, PUSH, SSL_PUSH, RADIUS, RDP, MYSQL, MSSQL, DIAMETER, SSL_DIAMETER, TFTP, ORACLE, SMPP, SYSLOGTCP, SYSLOGUDP, FIX, SSL_FIX, PROXY, USER_TCP, USER_SSL_TCP, QUIC, IPFIX, LOGSTREAM, MONGO, MONGO_TLS, MQTT, MQTT_TLS, QUIC_BRIDGE, HTTP_QUIC, DOT, SSL_PROXY, KAFKA_PRODUCER
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbsite_gslbservicegroup_binding/ sitename_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ gslbsite_gslbservicegroup_binding/ sitename_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of gslbsite_gslbservicegroup_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/gslbsite_gslbservicegroup_binding/ sitename_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the gslbsite_gslbservicegroup_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "gslbsite_gslbservicegroup_binding": [ {

"sitename":<String_value>,

"servicegroupname":<String_value>,

"servicetype":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbsite_gslbservicegroup_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/gslbsite_gslbservicegroup_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "gslbsite_gslbservicegroup_binding": [ {

"sitename":<String_value>,

"servicegroupname":<String_value>,

"servicetype":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbsite_gslbservicegroup_binding/ sitename_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"gslbsite_gslbservicegroup_binding": [ { "__count": "#no"} ] }
```

gslbsite_gslbservicegroupmember_binding

Binding object showing the gslbservicegroupmember that can be bound to gslbsite.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
servicegroupname	<String>	Read-write	Servicegroup name.
sitename	<String>	Read-write	Name of the GSLB site. If you specify a site name, details of all the site's constituent services are also displayed. Minimum length = 1
state	<String>	Read-only	State of the gslb service. Possible values = UP, DOWN, UNKNOWN, BUSY, OUT OF SERVICE, GOING OUT OF SERVICE, DOWN WHEN GOING OUT OF SERVICE, NS_EMPTY_STR, Unknown, DISABLED
port	<Integer>	Read-only	Port number of the gslb service. Range 1 - 65535 * in CLI is represented as 65535 in NITRO API

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
servicetype	<String>	Read-only	Service type. Possible values = HTTP, FTP, TCP, UDP, SSL, SSL_BRIDGE, SSL_TCP, DTLS, NNTP, DNS, DHCPRA, ANY, SIP_UDP, SIP_TCP, SIP_SSL, DNS_TCP, RTSP, PUSH, SSL_PUSH, RADIUS, RDP, MYSQL, MSSQL, DIAMETER, SSL_DIAMETER, TFTP, ORACLE, SMPP, SYSLOGTCP, SYSLOGUDP, FIX, SSL_FIX, PROXY, USER_TCP, USER_SSL_TCP, QUIC, IPFIX, LOGSTREAM, MONGO, MONGO_TLS, MQTT, MQTT_TLS, QUIC_BRIDGE, HTTP_QUIC, DOT, SSL_PROXY, KAFKA_PRODUCER
ipaddress	<String>	Read-only	IP Address of the gslb service.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbsite_gslbservicegroupmember_binding/ sitename_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ gslbsite_gslbservicegroupmember_binding/ sitename_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of gslbsite_gslbservicegroupmember_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ gslbsite_gslbservicegroupmember_binding/ sitename_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the gslbsite_gslbservicegroupmember_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "gslbsite_gslbservicegroupmember_binding": [ {

"servicegroupname":<String_value>,

"sitename":<String_value>,

"state":<String_value>,

"port":<Integer_value>,
```

```
"servicetype":<String_value>,

"ipaddress":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbsite_gslbservicegroupmember_binding
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/gslbsite_gslbservicegroupmember_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "gslbsite_gslbservicegroupmember_binding": [ {

"servicegroupname":<String_value>,

"sitename":<String_value>,

"state":<String_value>,
```

```
"port":<Integer_value>,

"servicetype":<String_value>,

"ipaddress":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbsite_gslbservicegroupmember_binding/ sitename_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"gslbsite_gslbservicegroupmember_binding": [ { "__count": "#no"} ] }
```

gslbsyncstatus

Configuration for sync status resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
summary	<Boolean>	Read-write	sync status summary to be displayed in one line (Success/ Failure), in case of Failure stating reason for failure.
response	<String>	Read-only	gslb sync status as text blob.
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbsyncstatus

Query-parameters:

args

http:// <netscaler-ip-address> /nitro/v1/config/gslbsyncstatus? **args=summary: <Boolean_value>**

Use this query-parameter to get gslbsyncstatus resources based on additional properties.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "gslbsyncstatus": [ {

summary:<Boolean_value>"response":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

gslbvserver

Configuration for Global Server Load Balancing Virtual Server resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the GSLB virtual server. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Can be changed after the virtual server is created. CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my vserver" or 'my vserver'). Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
servicetype	<String>	Read-write	Protocol used by services bound to the virtual server. Possible values = HTTP, FTP, TCP, UDP, SSL, SSL_BRIDGE, SSL_TCP, NNTP, ANY, SIP_UDP, SIP_TCP, SIP_SSL, RADIUS, RDP, RTSP, MYSQL, MSSQL, ORACLE
iptype	<String>	Read-write	The IP type for this GSLB vserver. Default value: IPV4 Possible values = IPV4, IPV6
dnsrecordtype	<String>	Read-write	DNS record type to associate with the GSLB virtual server's domain name. Default value: A Possible values = A, AAAA, CNAME, NAPTR
lbmethod	<String>	Read-write	Load balancing method for the GSLB virtual server. Default value: LEASTCONNECTION

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ROUNDROBIN, LEASTCONNECTION, LEASTRESPONSETIME, SOURCEIPHASH, LEASTBANDWIDTH, LEASTPACKETS, STATICPROXIMITY, RTT, CUSTOMLOAD, API
backupsessiontimeout	<Integer>	Read-write	A non zero value enables the feature whose minimum value is 2 minutes. The feature can be disabled by setting the value to zero. The created session is in effect for a specific client per domain. Minimum value = 0 Maximum value = 1440
backuplbmethod	<String>	Read-write	Backup load balancing method. Becomes operational if the primary load balancing method fails or cannot be used. Valid only if the primary method is

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			based on either round-trip time (RTT) or static proximity. Possible values = ROUNDROBIN, LEASTCONNECTION, LEASTRESPONSETIME, SOURCEIPHASH, LEASTBANDWIDTH, LEASTPACKETS, STATICPROXIMITY, RTT, CUSTOMLOAD, API
netmask	<String>	Read-write	IPv4 network mask for use in the SOURCEIPHASH load balancing method. Minimum length = 1
v6netmasklen	<Integer>	Read-write	Number of bits to consider, in an IPv6 source IP address, for creating the hash that is required by the SOURCEIPHASH load balancing method. Default value: 128 Minimum value = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum value = 128
rule	<String>	Read-write	Expression, or name of a named expression, against which traffic is evaluated. This field is applicable only if gslb method or gslb backup method are set to API. The following requirements apply only to the Citrix ADC CLI: * If the expression includes one or more spaces, enclose the entire expression in double quotation marks. * If the expression itself includes double quotation marks, escape the quotations by using the \ character. * Alternatively, you can use single quotation marks to enclose the rule, in

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			which case you do not have to escape the double quotation marks. Default value: "none"
tolerance	<Integer>	Read-write	Tolerance in milliseconds. Tolerance value is used in deciding which sites in a GSLB configuration must be considered for implementing the RTT load balancing method. The sites having the RTT value less than or equal to the sum of the lowest RTT and tolerance value are considered. NetScaler implements the round robin method of global server load balancing among these considered sites. The sites that have RTT value greater than this value are not considered. The logic is applied for each LDNS and based on the LDNS, the sites that are considered might change. For

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			example, a site that is considered for requests coming from LDNS1 might not be considered for requests coming from LDNS2. Minimum value = 0 Maximum value = 100
persistencetype	<String>	Read-write	Use source IP address based persistence for the virtual server. After the load balancing method selects a service for the first packet, the IP address received in response to the DNS query is used for subsequent requests from the same client. Possible values = SOURCEIP, NONE
persistenceid	<Integer>	Read-write	The persistence ID for the GSLB virtual server. The ID is a positive integer that enables GSLB sites to identify the GSLB virtual server, and is required if source IP address based or spill over based

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			persistence is enabled on the virtual server. Minimum value = 0 Maximum value = 65535
persistmask	<String>	Read-write	The optional IPv4 network mask applied to IPv4 addresses to establish source IP address based persistence. Minimum length = 1
v6persistmasklen	<Integer>	Read-write	Number of bits to consider in an IPv6 source IP address when creating source IP address based persistence sessions. Default value: 128 Minimum value = 1 Maximum value = 128
timeout	<Integer>	Read-write	Idle time, in minutes, after which a persistence entry is cleared. Default value: 2 Minimum value = 2 Maximum value = 1440

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
edr	<String>	Read-write	Send clients an empty DNS response when the GSLB virtual server is DOWN. Default value: DISABLED Possible values = ENABLED, DISABLED
ecs	<String>	Read-write	If enabled, respond with EDNS Client Subnet (ECS) option in the response for a DNS query with ECS. The ECS address will be used for persistence and spillover persistence (if enabled) instead of the LDNS address. Persistence mask is ignored if ECS is enabled. Default value: DISABLED Possible values = ENABLED, DISABLED
ecsaddrvalidation	<String>	Read-write	Validate if ECS address is a private or unroutable address and in such cases, use the LDNS IP.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: DISABLED Possible values = ENABLED, DISABLED
mir	<String>	Read-write	Include multiple IP addresses in the DNS responses sent to clients. Default value: DISABLED Possible values = ENABLED, DISABLED
disableprimaryondown	<String>	Read-write	Continue to direct traffic to the backup chain even after the primary GSLB virtual server returns to the UP state. Used when spillover is configured for the virtual server. Default value: DISABLED Possible values = ENABLED, DISABLED
dynamicweight	<String>	Read-write	Specify if the appliance should consider the service count, service weights, or ignore both when using

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			weight-based load balancing methods. The state of the number of services bound to the virtual server help the appliance to select the service. Default value: DISABLED Possible values = SERVICECOUNT, SERVICEWEIGHT, DISABLED
state	<String>	Read-write	State of the GSLB virtual server. Default value: ENABLED Possible values = ENABLED, DISABLED
considereffectivestate	<String>	Read-write	If the primary state of all bound GSLB services is DOWN, consider the effective states of all the GSLB services, obtained through the Metrics Exchange Protocol (MEP), when determining the state of the GSLB virtual server. To consider the effective state, set the parameter to

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			STATE_ONLY. To disregard the effective state, set the parameter to NONE. The effective state of a GSLB service is the ability of the corresponding virtual server to serve traffic. The effective state of the load balancing virtual server, which is transferred to the GSLB service, is UP even if only one virtual server in the backup chain of virtual servers is in the UP state. Default value: NONE Possible values = NONE, STATE_ONLY
comment	<String>	Read-write	Any comments that you might want to associate with the GSLB virtual server.
somethod	<String>	Read-write	Type of threshold that, when exceeded, triggers spillover. Available

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			settings function as follows: * CONNECTION - Spillover occurs when the number of client connections exceeds the threshold. * DYNAMICCONNECTION - Spillover occurs when the number of client connections at the GSLB virtual server exceeds the sum of the maximum client (Max Clients) settings for bound GSLB services. Do not specify a spillover threshold for this setting, because the threshold is implied by the Max Clients settings of the bound GSLB services. * BANDWIDTH - Spillover occurs when the bandwidth consumed by the GSLB virtual server's incoming

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			and outgoing traffic exceeds the threshold. * HEALTH - Spillover occurs when the percentage of weights of the GSLB services that are UP drops below the threshold. For example, if services gslbSvc1, gslbSvc2, and gslbSvc3 are bound to a virtual server, with weights 1, 2, and 3, and the spillover threshold is 50%, spillover occurs if gslbSvc1 and gslbSvc3 or gslbSvc2 and gslbSvc3 transition to DOWN. * NONE - Spillover does not occur. Possible values = CONNECTION, DYNAMICCONNECTION, BANDWIDTH, HEALTH, LLMQUOTA, NONE

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
sopersistence	<String>	Read-write	If spillover occurs, maintain source IP address based persistence for both primary and backup GSLB virtual servers. Default value: DISABLED Possible values = ENABLED, DISABLED
sopersistencetimeout	<Integer>	Read-write	Timeout for spillover persistence, in minutes. Default value: 2 Minimum value = 2 Maximum value = 1440
sothreshold	<Integer>	Read-write	Threshold at which spillover occurs. Specify an integer for the CONNECTION spillover method, a bandwidth value in kilobits per second for the BANDWIDTH method (do not enter the units), or a percentage for the HEALTH method (do not enter the percentage symbol). Minimum value = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum value = 4294967287
sobackupaction	<String>	Read-write	Action to be performed if spillover is to take effect, but no backup chain to spillover is usable or exists. Possible values = DROP, ACCEPT, REDIRECT
appflowlog	<String>	Read-write	Enable logging appflow flow information. Default value: ENABLED Possible values = ENABLED, DISABLED
toggleorder	<String>	Read-write	Configure this option to toggle order preference. Default value: ASCENDING Possible values = ASCENDING, DESCENDING
orderthreshold	<Integer>	Read-write	This option is used to to specify the threshold of minimum number of services to be UP in an order, for it to be

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			considered in Lb decision. Default value: 0 Minimum value = 0 Maximum value = 100
backupvserver	<String>	Read-write	Name of the backup GSLB virtual server to which the appliance should to forward requests if the status of the primary GSLB virtual server is down or exceeds its spillover threshold. Minimum length = 1
servicename	<String>	Read-write	Name of the GSLB service for which to change the weight. Minimum length = 1
weight	<Integer>	Read-write	Weight for the service. Minimum value = 1 Maximum value = 100
servicegroupname	<String>	Read-write	The GSLB service group name bound to the selected GSLB virtual server.
domainname	<String>	Read-write	Domain name for which to change the time to live (TTL)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			and/or backup service IP address. Minimum length = 1
ttl	<Integer>	Read-write	Time to live (TTL) for the domain. Minimum value = 1
backupip	<String>	Read-write	The IP address of the backup service for the specified domain name. Used when all the services bound to the domain are down, or when the backup chain of virtual servers is down. Minimum length = 1
cookie_domain	<String>	Read-write	The cookie domain for the GSLB site. Used when inserting the GSLB site cookie in the HTTP response. Minimum length = 1
cookietimeout	<Integer>	Read-write	Timeout, in minutes, for the GSLB site cookie. Minimum value = 0 Maximum value = 1440
sitedomainttl	<Integer>	Read-write	TTL, in seconds, for all internally created site domains (created when a site prefix is configured

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			on a GSLB service) that are associated with this virtual server. Minimum value = 1
order	<Integer>	Read-write	Order number to be assigned to the service when it is bound to the lb vserver. Minimum value = 1 Maximum value = 8192
newname	<String>	Read-write	New name for the GSLB virtual server. Minimum length = 1
curstate	<String>	Read-only	State of the gslb vserver. Possible values = UP, DOWN, UNKNOWN, BUSY, OUT OF SERVICE, GOING OUT OF SERVICE, DOWN WHEN GOING OUT OF SERVICE, NS_EMPTY_STR, Unknown, DISABLED
status	<Integer>	Read-only	Current status of the gslb vserver. During the initial phase if the configured lb method is not round robin ,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			the vserver will adopt round robin to distribute traffic for a predefined number of requests.
lbrrreason	<Integer>	Read-only	Reason why a vserver is in RR. The following are the reasons: 1 - MEP is DOWN (GSLB) 2 - LB method has changed 3 - Bound service's state changed to UP 4 - A new service is bound 5 - Startup RR factor has changed 6 - LB feature is enabled 7 - Load monitor is not active on a service 8 - Vserver is Enabled 9 - SSL feature is Enabled

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			10 - All bound services have reached threshold. Using effective state to load balance (GSLB) 11 - Primary state of bound services are not UP. Using effective state to load balance (GSLB) 12 - No LB decision can be made as all bound services have either reached threshold or are not UP (GSLB) 13 - All load monitors are active .
iscname	<String>	Read-only	is cname feature set on vserver. Possible values = ENABLED, DISABLED
sitepersistence	<String>	Read-only	Type of Site Persistence set. Possible values = ConnectionProxy, HTTPRedirect, NONE

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
totalservices	<Integer>	Read-only	Total number of services bound to the vserver.
activeservices	<Integer>	Read-only	Total number of active services bound to the vserver.
statechangetimesec	<String>	Read-only	Time when last state change happened. Seconds part.
statechangetimemsec	<Integer>	Read-only	Time at which last state change happened. Milliseconds part.
tickssincelaststatechange	<Integer>	Read-only	Time in 10 millisecond ticks since the last state change.
health	<Integer>	Read-only	Health of vserver based on percentage of weights of active svcs/all svcs. This does not consider administratively disabled svcs.
policyname	<String>	Read-only	Name of the policy bound to the GSLB vserver.
priority	<Integer>	Read-only	Priority. Minimum value = 1 Maximum value = 2147483647

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
gotopriorityexpression	<String>	Read-only	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE. o If gotoPriorityExpression is not present or if it is equal to END then the policy bank evaluation ends here o Else if the gotoPriorityExpression is equal to NEXT then the next policy in the priority order is evaluated. o Else gotoPriorityExpression is evaluated. The result of gotoPriorityExpression (which has to be a number) is processed as follows: - An UNDEF event is triggered if . gotoPriorityExpressi

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			on cannot be evaluated . gotoPriorityExpression evaluates to number which is smaller than the maximum priority in the policy bank but is not same as any policy's priority . gotoPriorityExpression evaluates to a priority that is smaller than the current policy's priority - If the gotoPriorityExpression evaluates to the priority of the current policy then the next policy in the priority order is evaluated. - If the gotoPriorityExpression evaluates to the priority of a policy further ahead in the list then that policy

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			will be evaluated next. This field is applicable only to rewrite and responder policies.
type	<String>	Read-only	The bindpoint to which the policy is bound. Possible values = REQUEST, RESPONSE, MQTT_JUMBO_REQ
vsvrbindsvcip	<String>	Read-only	used for showing the ip of bound entities.
vsvrbindsvcport	<Integer>	Read-only	used for showing ports of bound entities. Range 1 - 65535 * in CLI is represented as 65535 in NITRO API
servername	<String>	Read-only	This field is used to display server name in case of GSLB servicegroup binding to GSLB vserver .
nodefaultbindings	<String>	Read-only	to determine if the configuration will have default ssl

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			CIPHER and ECC curve bindings. Default value: NO Possible values = YES, NO
currentactiveorder	<String>	Read-only	current order that takes the traffic in case service or servicegroup is bound with order.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- ENABLE
- DISABLE
- GET (ALL)
- GET
- COUNT
- RENAME

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbvserver **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"gslbvserver":{

<b>"name":<String_value>,

</b><b>"servicetype":<String_value>,

</b>"iptype":<String_value>,

"dnsrecordtype":<String_value>,

"lbmethod":<String_value>,
```

```
"backupsessiontimeout":<Integer_value>,

"backuplbmethod":<String_value>,

"netmask":<String_value>,

"v6netmasklen":<Integer_value>,

"rule":<String_value>,

"tolerance":<Integer_value>,

"persistencetype":<String_value>,

"persistenceid":<Integer_value>,

"persistmask":<String_value>,

"v6persistmasklen":<Integer_value>,

"timeout":<Integer_value>,

"edr":<String_value>,

"ecs":<String_value>,

"ecsaddrvalidation":<String_value>,

"mir":<String_value>,

"disableprimaryondown":<String_value>,

"dynamicweight":<String_value>,

"state":<String_value>,

"considereffectivestate":<String_value>,

"comment":<String_value>,

"somethod":<String_value>,

"sopersistence":<String_value>,
```

```
"sopersistencetimeout":<Integer_value>,

"sothreshold":<Integer_value>,

"sobackupaction":<String_value>,

"appflowlog":<String_value>,

"toggleorder":<String_value>,

"orderthreshold":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbvserver/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbvserver **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"gslbvserver":{

<b>"name":<String_value>,

</b>"iptype":<String_value>,

"dnsrecordtype":<String_value>,

"backupvserver":<String_value>,

"backupsessiontimeout":<Integer_value>,

"lbmethod":<String_value>,

"backuplbmethod":<String_value>,

"netmask":<String_value>,

"v6netmasklen":<Integer_value>,

"tolerance":<Integer_value>,

"persistencetype":<String_value>,

"persistenceid":<Integer_value>,

"persistmask":<String_value>,

"v6persistmasklen":<Integer_value>,

"timeout":<Integer_value>,

"edr":<String_value>,

"ecs":<String_value>,

"ecsaddrvalidation":<String_value>,

"mir":<String_value>,

"disableprimaryondown":<String_value>,

"dynamicweight":<String_value>,
```

```
"considereffectivestate":<String_value>,

"somethod":<String_value>,

"sopersistence":<String_value>,

"sopersistencetimeout":<Integer_value>,

"sothreshold":<Integer_value>,

"sobackupaction":<String_value>,

"servicename":<String_value>,

"weight":<Integer_value>,

"servicegroupname":<String_value>,

"domainname":<String_value>,

"ttl":<Integer_value>,

"backupip":<String_value>,

"cookie_domain":<String_value>,

"cookietimeout":<Integer_value>,

"sitedomainttl":<Integer_value>,

"comment":<String_value>,

"appflowlog":<String_value>,

"rule":<String_value>,

"togglorder":<String_value>,

"orderthreshold":<Integer_value>,

"order":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbvserver? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"gslbvserver":{

<b>"name":<String_value>,

</b>"backupvserver":true,

"sothreshold":true,

"servicename":true,

"servicegroupname":true,

"order":true,

"iptype":true,

"dnsrecordtype":true,

"backupsessiontimeout":true,

"lbmethod":true,

"backuplbmethod":true,
```

```
"netmask":true,

"v6netmasklen":true,

"tolerance":true,

"persistencetype":true,

"persistenceid":true,

"persistmask":true,

"v6persistmasklen":true,

"timeout":true,

"edr":true,

"ecs":true,

"ecsaddrvalidation":true,

"mir":true,

"disableprimaryondown":true,

"dynamicweight":true,

"considereffectivestate":true,

"somethod":true,

"sopersistence":true,

"sopersistencetimeout":true,

"sobackupaction":true,

"weight":true,

"comment":true,

"appflowlog":true,
```

```
"rule":true,

"togglеorder":true,

"orderthreshold":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

ENABLE

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbvserver? **action=enable HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"gslbvserver":{

<b>"name":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DISABLE

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbvserver? **action=disable HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"gslbvserver":{

<b>"name":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

RENAME

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbvserver? **action=rename HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"gslbvserver":{

<b>"name":<String_value>,

</b><b>"newname":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbvserver **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/gslbvserver? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/gslbvserver? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of gslbvserver resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/gslbvserver? **view=summary**

Use this query-parameter to get the summary output of gslbvserver resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/gslbvserver? **pagesize=#no;pageno=#no**

Use this query-parameter to get the gslbvserver resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "gslbvserver": [ {

"name":<String_value>,

"servicetype":<String_value>,

"state":<String_value>,

"iptype":<String_value>,

"dnsrecordtype":<String_value>,

"persistencetype":<String_value>,

"persistenceid":<Integer_value>,

"lbmethod":<String_value>,

"backuplbmethod":<String_value>,

"tolerance":<Integer_value>,

"timeout":<Integer_value>,

"curstate":<String_value>,

"netmask":<String_value>,

"v6netmasklen":<Integer_value>,

"persistmask":<String_value>,

"v6persistmasklen":<Integer_value>,

"servicename":<String_value>,

"weight":<Integer_value>,

"domainname":<String_value>,

"ttl":<Integer_value>,

"backupip":<String_value>,
```

```
"cookie_domain":<String_value>,

"cookietimeout":<Integer_value>,

"sitedomainttl":<Integer_value>,

"status":<Integer_value>,

"lbrrreason":<Integer_value>,

"backupvserver":<String_value>,

"backupsessiontimeout":<Integer_value>,

"edr":<String_value>,

"ecs":<String_value>,

"ecsaddrvalidation":<String_value>,

"mir":<String_value>,

"disableprimaryondown":<String_value>,

"dynamicweight":<String_value>,

"iscname":<String_value>,

"sitepersistence":<String_value>,

"considereffectivestate":<String_value>,

"totalservices":<Integer_value>,

"activeservices":<Integer_value>,

"statechangetimesec":<String_value>,

"statechangetimemsec":<Integer_value>,

"tickssincelaststatechange":<Integer_value>,

"comment":<String_value>,
```

```
"sopersistencetimeout":<Integer_value>,

"somethod":<String_value>,

"sobackupaction":<String_value>,

"sopersistence":<String_value>,

"sothreshold":<Integer_value>,

"health":<Integer_value>,

"appflowlog":<String_value>,

"policyname":<String_value>,

"priority":<Integer_value>,

"gotopriorityexpression":<String_value>,

"type":<String_value>,

"vsvrbindsvcip":<String_value>,

"vsvrbindsvcport":<Integer_value>,

"servername":<String_value>,

"servicegroupname":<String_value>,

"nodefaultbindings":<String_value>,

"rule":<String_value>,

"order":<Integer_value>,

"toggleorder":<String_value>,

"orderthreshold":<Integer_value>,

"currentactiveorder":<String_value>,

"_nextgenapiresource":<String_value>
```

```
}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbvserver/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/gslbvserver/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/gslbvserver/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of gslbvserver resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "gslbvserver": [ {

"name":<String_value>,

"servicetype":<String_value>,
```

```
"state":<String_value>,

"iptype":<String_value>,

"dnsrecordtype":<String_value>,

"persistencetype":<String_value>,

"persistenceid":<Integer_value>,

"lbmethod":<String_value>,

"backuplbmethod":<String_value>,

"tolerance":<Integer_value>,

"timeout":<Integer_value>,

"curstate":<String_value>,

"netmask":<String_value>,

"v6netmasklen":<Integer_value>,

"persistmask":<String_value>,

"v6persistmasklen":<Integer_value>,

"servicename":<String_value>,

"weight":<Integer_value>,

"domainname":<String_value>,

"ttl":<Integer_value>,

"backupip":<String_value>,

"cookie_domain":<String_value>,

"cookietimeout":<Integer_value>,

"sitedomainttl":<Integer_value>,
```

```
"status":<Integer_value>,

"lbrrreason":<Integer_value>,

"backupvserver":<String_value>,

"backupsessiontimeout":<Integer_value>,

"edr":<String_value>,

"ecs":<String_value>,

"ecsaddrvalidation":<String_value>,

"mir":<String_value>,

"disableprimaryondown":<String_value>,

"dynamicweight":<String_value>,

"iscname":<String_value>,

"sitepersistence":<String_value>,

"considereffectivestate":<String_value>,

"totalservices":<Integer_value>,

"activeservices":<Integer_value>,

"statechangetimesec":<String_value>,

"statechangetimemsec":<Integer_value>,

"tickssincelaststatechange":<Integer_value>,

"comment":<String_value>,

"sopersistencetimeout":<Integer_value>,

"somethod":<String_value>,

"sobackupaction":<String_value>,
```

```
"sopersistence":<String_value>,

"sothreshold":<Integer_value>,

"health":<Integer_value>,

"appflowlog":<String_value>,

"policyname":<String_value>,

"priority":<Integer_value>,

"gotopriorityexpression":<String_value>,

"type":<String_value>,

"vsvrbindsvcip":<String_value>,

"vsvrbindsvcport":<Integer_value>,

"servername":<String_value>,

"servicegroupname":<String_value>,

"nodefaultbindings":<String_value>,

"rule":<String_value>,

"order":<Integer_value>,

"toggleorder":<String_value>,

"orderthreshold":<Integer_value>,

"currentactiveorder":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbvserver? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "gslbvserver": [ { "__count": "#no"} ] }
```

gslbvserver_binding

Binding object which returns the resources bound to gslbvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the GSLB virtual server. Minimum length = 1
gslbvserver_domain_binding	<gslbvserver_domain_binding[]>	Read-only	domain that can be bound to gslbvserver.
gslbvserver_spillover policy_binding	<gslbvserver_spillover policy_binding[]>	Read-only	spilloverpolicy that can be bound to gslbvserver.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
gslbvserver_gslbservicegroup_binding	<gslbvserver_gslbservicegroup_binding[]>	Read-only	gslbservicegroup that can be bound to gslbvserver.
gslbvserver_lbpolicy_binding	<gslbvserver_lbpolicy_binding[]>	Read-only	lbpolicy that can be bound to gslbvserver.
gslbvserver_gslbservice_binding	<gslbvserver_gslbservice_binding[]>	Read-only	gslbservice that can be bound to gslbvserver.
gslbvserver_gslbservicegroupmember_binding	<gslbvserver_gslbservicegroupmember_binding[]>	Read-only	gslbservicegroupmember that can be bound to gslbvserver.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbvserver_binding/ name_value<String>
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "gslbvserver_binding": [ {

"name":<String_value>,

"gslbvserver_gslbservice_binding":<gslbvserver_gslbservice_binding[]_value
>,

"gslbvserver_gslbservicegroup_binding":<gslbvserver_gslbservicegroup_bindi
ng[]_value>,

"gslbvserver_gslbservicegroupmember_binding":<gslbvserver_gslbservicegroup
```

```
member_binding[]_value>,

"gslbvserver_lbpolicy_binding":<gslbvserver_lbpolicy_binding[]_value>,

"gslbvserver_domain_binding":<gslbvserver_domain_binding[]_value>,

"gslbvserver_spilloverpolicy_binding":<gslbvserver_spilloverpolicy_binding
[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbvserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/gslbvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "gslbvserver_binding": [ {

"name":<String_value>,

"gslbvserver_gslbservice_binding":<gslbvserver_gslbservice_binding[]_value
```

```
>,

"gslbvserver_gslbservicegroup_binding":<gslbvserver_gslbservicegroup_bindi
ng[]_value>,

"gslbvserver_gslbservicegroupmember_binding":<gslbvserver_gslbservicegroup
member_binding[]_value>,

"gslbvserver_lbpolicy_binding":<gslbvserver_lbpolicy_binding[]_value>,

"gslbvserver_domain_binding":<gslbvserver_domain_binding[]_value>,

"gslbvserver_spilloverpolicy_binding":<gslbvserver_spilloverpolicy_binding
[]_value>

}]}
```

gslbvserver_domain_binding

Binding object showing the domain that can be bound to gslbvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ttl	<Integer>	Read-write	Time to live (TTL) for the domain. Minimum value = 1
cookie_domain	<String>	Read-write	The cookie domain for the GSLB site. Used when inserting the GSLB site cookie in the HTTP response. Minimum length = 1
domainname	<String>	Read-write	Domain name for which to change the time to live (TTL)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			and/or backup service IP address. Minimum length = 1
order	<Integer>	Read-write	Order number to be assigned to the service when it is bound to the lb vserver. Minimum value = 1 Maximum value = 8192
cookie_domainflag	<Boolean>	Read-write	The cookie domain for the GSLB site. Used when inserting the GSLB site cookie in the HTTP response.
backupip	<String>	Read-write	The IP address of the backup service for the specified domain name. Used when all the services bound to the domain are down, or when the backup chain of virtual servers is down. Minimum length = 1
backupipflag	<Boolean>	Read-write	The IP address of the backup service for the specified domain name. Used when all the services bound to the domain are down, or when the backup chain of

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			virtual servers is down.
cookietimeout	<Integer>	Read-write	Timeout, in minutes, for the GSLB site cookie. Minimum value = 0 Maximum value = 1440
sitedomainttl	<Integer>	Read-write	TTL, in seconds, for all internally created site domains (created when a site prefix is configured on a GSLB service) that are associated with this virtual server. Minimum value = 1
name	<String>	Read-write	Name of the virtual server on which to perform the binding operation. Minimum length = 1
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/gslbvserver_domain_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"gslbvserver_domain_binding":{
```

```
<b>"name":<String_value>,

</b>"domainname":<String_value>,

"ttl":<Integer_value>,

"backupip":<String_value>,

"cookie_domain":<String_value>,

"cookietimeout":<Integer_value>,

"sitedomainttl":<Integer_value>,

"order":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbvserver_domain_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ gslbvserver_domain_binding/ name_value<String> ? **args=domainname: <String_value> ,backupipflag: <Boolean_value> ,cookie_domainflag: <Boolean_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbvserver_domain_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ gslbvserver_domain_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of gslbvserver_domain_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/gslbvserver_domain_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the gslbvserver_domain_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "gslbvserver_domain_binding": [ {

"ttl":<Integer_value>,

"cookie_domain":<String_value>,

"domainname":<String_value>,

"order":<Integer_value>,

"cookie_domainflag":<Boolean_value>,
```

```
"backupip":<String_value>,

"backupipflag":<Boolean_value>,

"cookietimeout":<Integer_value>,

"sitedomainttl":<Integer_value>,

"name":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbvserver_domain_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/gslbvserver_domain_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "gslbvserver_domain_binding": [ {

"ttl":<Integer_value>,

"cookie_domain":<String_value>,

"domainname":<String_value>,

"order":<Integer_value>,

"cookie_domainflag":<Boolean_value>,

"backupip":<String_value>,

"backupipflag":<Boolean_value>,

"cookietimeout":<Integer_value>,

"sitedomainttl":<Integer_value>,

"name":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbvserver_domain_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"gslbvserver_domain_binding": [ { "__count": "#no"} ] }
```

gslbvserver_gslbservice_binding

Binding object showing the gslbservice that can be bound to gslbvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
servicename	<String>	Read-write	Name of the GSLB service for which to change the weight. Minimum length = 1
domainname	<String>	Read-write	Domain name for which to change the time to live (TTL) and/or backup service IP address. Minimum length = 1
order	<Integer>	Read-write	Order number to be assigned to the service when it is bound to the lb vserver. Minimum value = 1 Maximum value = 8192
name	<String>	Read-write	Name of the virtual server on which to perform the binding operation. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
weight	<Integer>	Read-write	Weight for the service. Minimum value = 1 Maximum value = 100
gslbthreshold	<Integer>	Read-only	Indicates if gslb svc has reached threshold.
thresholdvalue	<Integer>	Read-only	Tells whether threshold exceeded for this service participating in CUSTOMLB.
orderstr	<String>	Read-only	Order number in string form assigned to the service when it is bound to the lb vserver.
dynamicconfwt	<Integer>	Read-only	Weight obtained by the virtue of bound service count or weight.
svreffgslbstate	<String>	Read-only	Effective state of the gslb svc. Possible values = UP, DOWN, UNKNOWN, BUSY, OUT OF SERVICE, GOING OUT OF SERVICE, DOWN WHEN GOING OUT OF SERVICE, NS_EMPTY_STR,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Unknown, DISABLED
preferredlocation	<String>	Read-only	The target site to be returned in the DNS response when a policy is successfully evaluated against the incoming DNS request. Target site is specified in dotted notation with up to 6 qualifiers. Wildcard `*' is accepted as a valid qualifier token.
iscname	<String>	Read-only	is cname feature set on vserver. Possible values = ENABLED, DISABLED
gslbboundsvctype	<String>	Read-only	Protocol used by services bound to the GSLBvirtual server. Possible values = HTTP, FTP, TCP, UDP, SSL, SSL_BRIDGE, SSL_TCP, NNTP, ANY, SIP_UDP, SIP_TCP, SIP_SSL, RADIUS, RDP, RTSP, MYSQL, MSSQL, ORACLE
cnameentry	<String>	Read-only	The cname of the gslb service.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
svcsitepersistence	<String>	Read-only	Type of Site Persistence set on the bound service. Possible values = ConnectionProxy, HTTPRedirect, NONE
cumulativeweight	<Integer>	Read-only	Cumulative weight is the weight of GSLB service considering both its configured weight and dynamic weight. It is equal to product of dynamic weight and configured weight of the gslb service .
port	<Integer>	Read-only	Port number. Range 1 - 65535 * in CLI is represented as 65535 in NITRO API
ipaddress	<String>	Read-only	IP address.
sitepersistcookie	<String>	Read-only	This field is introduced for displaying the cookie in cluster setup. Minimum length = 1
curstate	<String>	Read-only	State of the gslb vserver. Possible values = UP, DOWN, UNKNOWN, BUSY,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			OUT OF SERVICE, GOING OUT OF SERVICE, DOWN WHEN GOING OUT OF SERVICE, NS_EMPTY_STR, Unknown, DISABLED
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/gslbvserver_gslbservice_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"gslbvserver_gslbservice_binding":{

<b>"name":<String_value>,

</b>"servicename":<String_value>,

"weight":<Integer_value>,

"domainname":<String_value>,

"order":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbvserver_gslbservice_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ gslbvserver_gslbservice_binding/ name_value<String> ? **args=servicename: <String_value> ,domainname: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbvserver_gslbservice_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ gslbvserver_gslbservice_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of gslbvserver_gslbservice_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/gslbvserver_gslbservice_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the gslbvserver_gslbservice_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "gslbvserver_gslbservice_binding": [ {

"servicename":<String_value>,

"domainname":<String_value>,

"order":<Integer_value>,

"name":<String_value>,

"weight":<Integer_value>,

"gslbthreshold":<Integer_value>,

"thresholdvalue":<Integer_value>,

"orderstr":<String_value>,

"dynamicconfwt":<Integer_value>,

"svreffgslbstate":<String_value>,

"preferredlocation":<String_value>,

"iscname":<String_value>,

"gslbboundsvctype":<String_value>,

"cnameentry":<String_value>,

"svcsitepersistence":<String_value>,

"cumulativeweight":<Integer_value>,

"port":<Integer_value>,

"ipaddress":<String_value>,
```

```
"sitepersistcookie":<String_value>,

"curstate":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbvserver_gslbservice_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/gslbvserver_gslbservice_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "gslbvserver_gslbservice_binding": [ {

"servicename":<String_value>,

"domainname":<String_value>,

"order":<Integer_value>,
```

```
"name":<String_value>,

"weight":<Integer_value>,

"gslbthreshold":<Integer_value>,

"thresholdvalue":<Integer_value>,

"orderstr":<String_value>,

"dynamicconfwt":<Integer_value>,

"svreffgslbstate":<String_value>,

"preferredlocation":<String_value>,

"iscname":<String_value>,

"gslbboundsvctype":<String_value>,

"cnameentry":<String_value>,

"svcsitepersistence":<String_value>,

"cumulativeweight":<Integer_value>,

"port":<Integer_value>,

"ipaddress":<String_value>,

"sitepersistcookie":<String_value>,

"curstate":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbvserver_gslbservice_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"gslbvserver_gslbservice_binding": [ { "__count": "#no"} ] }
```

gslbvserver_gslbservicegroup_binding

Binding object showing the gslbservicegroup that can be bound to gslbvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
order	<Integer>	Read-write	Order number to be assigned to the service when it is bound to the lb vserver. Minimum value = 1 Maximum value = 8192
servicegroupname	<String>	Read-write	The GSLB service group name bound to the selected GSLB virtual server.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the virtual server on which to perform the binding operation. Minimum length = 1
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/gslbvserver_gslbservicegroup_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"gslbvserver_gslbservicegroup_binding":{

<b>"name":<String_value>,

</b>"servicegroupname":<String_value>,

"order":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbvserver_gslbservicegroup_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ gslbvserver_gslbservicegroup_binding/ name_value<String> ? **args=servicegroupname: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbvserver_gslbservicegroup_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ gslbvserver_gslbservicegroup_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of gslbvserver_gslbservicegroup_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/gslbvserver_gslbservicegroup_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the gslbvserver_gslbservicegroup_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "gslbvserver_gslbservicegroup_binding": [ {

"order":<Integer_value>,

"servicegroupname":<String_value>,

"name":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbvserver_gslbservicegroup_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/gslbvserver_gslbservicegroup_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "gslbvserver_gslbservicegroup_binding": [ {

"order":<Integer_value>,
```

```
"servicegroupname":<String_value>,

"name":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbvserver_gslbservicegroup_binding/name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"gslbvserver_gslbservicegroup_binding": [ { "__count": "#no"} ] }
```

gslbvserver_gslbservicegroupmember_binding

Binding object showing the gslbservicegroupmember that can be bound to gslbvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
order	<Integer>	Read-write	Order number to be assigned to the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			service when it is bound to the lb vserver. Minimum value = 1 Maximum value = 8192
weight	<Integer>	Read-write	Weight for the service. Minimum value = 1 Maximum value = 100
servicegroupname	<String>	Read-write	The GSLB service group name bound to the selected GSLB virtual server.
name	<String>	Read-write	Name of the virtual server on which to perform the binding operation. Minimum length = 1
dynamicweight	<String>	Read-only	Specify if the appliance should consider the service count, service weights, or ignore both when using weight-based load balancing methods. The state of the number of services bound to the virtual server help the appliance to select the service.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: DISABLED Possible values = SERVICECOUNT, SERVICEWEIGHT, DISABLED
orderstr	<String>	Read-only	Order number in string form assigned to the service when it is bound to the lb vserver.
thresholdvalue	<Integer>	Read-only	Tells whether threshold exceeded for this service participating in CUSTOMLB.
gslbthreshold	<Integer>	Read-only	Indicates if gslb svc has reached threshold.
svreffgslbstate	<String>	Read-only	Effective state of the gslb svc. Possible values = UP, DOWN, UNKNOWN, BUSY, OUT OF SERVICE, GOING OUT OF SERVICE, DOWN WHEN GOING OUT OF SERVICE, NS_EMPTY_STR, Unknown, DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
preferredlocation	<String>	Read-only	The target site to be returned in the DNS response when a policy is successfully evaluated against the incoming DNS request. Target site is specified in dotted notation with up to 6 qualifiers. Wildcard `*' is accepted as a valid qualifier token.
svcsitepersistence	<String>	Read-only	Type of Site Persistence set on the bound service. Possible values = ConnectionProxy, HTTPRedirect, NONE
sitepersistcookie	<String>	Read-only	This field is introduced for displaying the cookie in cluster setup. Minimum length = 1
ipaddress	<String>	Read-only	IP address.
curstate	<String>	Read-only	State of the gslb vserver. Possible values = UP, DOWN, UNKNOWN, BUSY, OUT OF SERVICE, GOING OUT OF SERVICE, DOWN WHEN GOING OUT OF SERVICE,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			NS_EMPTY_STR, Unknown, DISABLED
servicetype	<String>	Read-only	Protocol used by services bound to the virtual server. Possible values = HTTP, FTP, TCP, UDP, SSL, SSL_BRIDGE, SSL_TCP, NNTP, ANY, SIP_UDP, SIP_TCP, SIP_SSL, RADIUS, RDP, RTSP, MYSQL, MSSQL, ORACLE
port	<Integer>	Read-only	Port number. Range 1 - 65535 * in CLI is represented as 65535 in NITRO API
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbvserver_gslbservicegroupmember_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ gslbvserver_gslbservicegroupmember_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of gslbvserver_gslbservicegroupmember_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ gslbvserver_gslbservicegroupmember_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the gslbvserver_gslbservicegroupmember_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "gslbvserver_gslbservicegroupmember_binding": [ {

"order":<Integer_value>,

"weight":<Integer_value>,

"servicegroupname":<String_value>,

"name":<String_value>,

"dynamicweight":<String_value>,

"orderstr":<String_value>,

"thresholdvalue":<Integer_value>,

"gslbthreshold":<Integer_value>,

"svreffgslbstate":<String_value>,

"preferredlocation":<String_value>,

"svcsitepersistence":<String_value>,

"sitepersistcookie":<String_value>,

"ipaddress":<String_value>,
```

```
"curstate":<String_value>,

"servicetype":<String_value>,

"port":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbvserver_gslbservicegroupmember_binding
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/gslbvserver_gslbservicegroupmember_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "gslbvserver_gslbservicegroupmember_binding": [ {

"order":<Integer_value>,

"weight":<Integer_value>,
```

```
"servicegroupname":<String_value>,

"name":<String_value>,

"dynamicweight":<String_value>,

"orderstr":<String_value>,

"thresholdvalue":<Integer_value>,

"gslbthreshold":<Integer_value>,

"svreffgslbstate":<String_value>,

"preferredlocation":<String_value>,

"svcsitepersistence":<String_value>,

"sitepersistcookie":<String_value>,

"ipaddress":<String_value>,

"curstate":<String_value>,

"servicetype":<String_value>,

"port":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbvserver_gslbservicegroupmember_binding/name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"gslbvserver_gslbservicegroupmember_binding": [ { "__count": "#no"} ] }
```

gslbvserver_lbpolicy_binding

Binding object showing the lbpolicy that can be bound to gslbvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
type	<String>	Read-write	The bindpoint to which the policy is bound. Possible values = REQUEST, RESPONSE, MQTT_JUMBO_REQ
gotopriorityexpression	<String>	Read-write	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE. o If gotoPriorityExpression is not present or if it is equal to END then the policy bank

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			evaluation ends here o Else if the gotoPriorityExpression is equal to NEXT then the next policy in the priority order is evaluated. o Else gotoPriorityExpression is evaluated. The result of gotoPriorityExpression (which has to be a number) is processed as follows: - An UNDEF event is triggered if . gotoPriorityExpression cannot be evaluated . gotoPriorityExpression evaluates to number which is smaller than the maximum priority in the policy bank but is not same as any policy's priority . gotoPriorityExpression evaluates to a priority that is smaller than the current policy's priority - If the gotoPriorityExpression evaluates to the priority of the current policy then the next policy in the priority order is evaluated. - If the gotoPriorityExpressio

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			n evaluates to the priority of a policy further ahead in the list then that policy will be evaluated next. This field is applicable only to rewrite and responder policies.
policyname	<String>	Read-write	Name of the policy bound to the GSLB vserver.
name	<String>	Read-write	Name of the virtual server on which to perform the binding operation. Minimum length = 1
priority	<Integer>	Read-write	Priority. Minimum value = 1 Maximum value = 2147483647
order	<Integer>	Read-write	Order number to be assigned to the service when it is bound to the lb vserver. Minimum value = 1 Maximum value = 8192
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/gslbvserver_lbpolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"gslbvserver_lbpolicy_binding":{

<b>"name":<String_value>,

</b>"policyname":<String_value>,

"priority":<Integer_value>,

"gotopriorityexpression":<String_value>,

"type":<String_value>,

"order":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbvserver_lbpolicy_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ gslbvserver_lbpolicy_binding/ name_value<String> ? **args=policyname: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbvserver_lbpolicy_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ gslbvserver_lbpolicy_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of gslbvserver_lbpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/gslbvserver_lbpolicy_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the gslbvserver_lbpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "gslbvserver_lbpolicy_binding": [ {

"type":<String_value>,

"gotopriorityexpression":<String_value>,

"policyname":<String_value>,

"name":<String_value>,

"priority":<Integer_value>,
```

```
"order":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbvserver_lbpolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/gslbvserver_lbpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "gslbvserver_lbpolicy_binding": [ {

"type":<String_value>,

"gotopriorityexpression":<String_value>,

"policyname":<String_value>,

"name":<String_value>,
```

```
"priority":<Integer_value>,

"order":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbvserver_lbpolicy_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"gslbvserver_lbpolicy_binding": [ { "__count": "#no"} ] }
```

gslbvserver_spilloverpolicy_binding

Binding object showing the spilloverpolicy that can be bound to gslbvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
priority	<Integer>	Read-write	Priority.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum value = 1 Maximum value = 2147483647
name	<String>	Read-write	Name of the virtual server on which to perform the binding operation. Minimum length = 1
order	<Integer>	Read-write	Order number to be assigned to the service when it is bound to the lb vserver. Minimum value = 1 Maximum value = 8192
type	<String>	Read-write	The bindpoint to which the policy is bound. Possible values = REQUEST, RESPONSE, MQTT_JUMBO_REQ
gotopriorityexpression	<String>	Read-write	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE. o If gotoPriorityExpression is not present or if

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			it is equal to END then the policy bank evaluation ends here o Else if the gotoPriorityExpression is equal to NEXT then the next policy in the priority order is evaluated. o Else gotoPriorityExpression is evaluated. The result of gotoPriorityExpression (which has to be a number) is processed as follows: - An UNDEF event is triggered if . gotoPriorityExpression cannot be evaluated . gotoPriorityExpression evaluates to number which is smaller than the maximum priority in the policy bank but is not same as any policy's priority . gotoPriorityExpression evaluates to a priority that is smaller than the current policy's priority - If the gotoPriorityExpression evaluates to the priority of the current policy then the next policy in the priority order is evaluated. -

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			If the gotoPriorityExpression evaluates to the priority of a policy further ahead in the list then that policy will be evaluated next. This field is applicable only to rewrite and responder policies.
policyname	<String>	Read-write	Name of the policy bound to the GSLB vserver.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/gslbvserver_spilloverpolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"gslbvserver_spilloverpolicy_binding":{

<b>"name":<String_value>,

</b>"policyname":<String_value>,

"priority":<Integer_value>,

"gotopriorityexpression":<String_value>,

"type":<String_value>,
```

```
"order":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbvserver_spilloverpolicy_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ gslbvserver_spilloverpolicy_binding/ name_value<String> ? **args=policyname: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbvserver_spilloverpolicy_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ gslbvserver_spilloverpolicy_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of gslbvserver_spilloverpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/gslbvserver_spilloverpolicy_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the gslbvserver_spilloverpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "gslbvserver_spilloverpolicy_binding": [ {

"priority":<Integer_value>,

"name":<String_value>,

"order":<Integer_value>,

"type":<String_value>,

"gotopriorityexpression":<String_value>,

"policyname":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbvserver_spilloverpolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/gslbvserver_spilloverpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "gslbvserver_spilloverpolicy_binding": [ {

"priority":<Integer_value>,

"name":<String_value>,

"order":<Integer_value>,

"type":<String_value>,

"gotopriorityexpression":<String_value>,

"policyname":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/gslbvserver_spilloverpolicy_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"gslbvserver_spilloverpolicy_binding": [ { "__count": "#no"} ] }
```

ha

High Availability

High-availability commands.

NAME	DESCRIPTION
hafailover	Configuration for failover
hafiles	Configuration for files
hanode	Configuration for node
hanode_binding	Binding object showing the resources that can be bound to hanode
hanode_ci_binding	Binding object showing the ci that can be bound to hanode
hanode_fis_binding	Binding object showing the fis that can be bound to hanode

NAME	DESCRIPTION
hanode_partialfailureinterfaces_binding	Binding object showing the partialfailureinterfaces that can be bound to hanode
hanode_routemonitor6_binding	Binding object showing the routemonitor6 that can be bound to hanode
hanode_routemonitor_binding	Binding object showing the routemonitor that can be bound to hanode
hasync	Configuration for sync
hasyncfailures	Configuration for HA sync failures

hafailover

Configuration for failover resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
force	<Boolean>	Read-write	Force a failover without prompting for confirmation.

Operations

(click to see Properties)

- FORCE

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

FORCE

URL: http:// <netscaler-ip-address> /nitro/v1/config/hafailover? **action=Force**

HTTP Method: POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"hafailover":{

"force":<Boolean_value>

}}
```

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

hafiles

Configuration for files resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
mode	<String[]>	Read-write	Specify one of the following modes of synchronization. * all - Synchronize files related to system configuration, Access Gateway bookmarks, SSL certificates, SSL CRL lists, and Application Firewall XML objects. * bookmarks - Synchronize all Access Gateway bookmarks.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			* ssl - Synchronize all certificates, keys, and CRLs for the SSL feature. * imports. Synchronize all XML objects (for example, WSDLs, schemas, error pages) configured for the application firewall. * misc - Synchronize all license files and the rc.conf file. * all_plus_misc - Synchronize files related to system configuration, Access Gateway bookmarks, SSL certificates, SSL CRL lists, application firewall XML objects, licenses, and the rc.conf file. Possible values = all, bookmarks, ssl, imports, misc, dns, krb, AAA, app_catalog,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			all_plus_misc, all_minus_misc

Operations

(click to see Properties)

- SYNC

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

SYNC

URL: http:// <netscaler-ip-address> /nitro/v1/config/hafiles? **action=sync HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"hafiles":{

"mode":<String[]_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

hanode

Configuration for node resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
id	<Integer>	Read-write	Number that uniquely identifies the node. For self node, it will always be 0. Peer node values can range from 1-64. Minimum value = 1 Maximum value = 64
ipaddress	<String>	Read-write	The NSIP or NSIP6 address of the node to be added for an HA configuration.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			This setting is neither propagated nor synchronized. Minimum length = 1
inc	<String>	Read-write	This option is required if the HA nodes reside on different networks. When this mode is enabled, the following independent network entities and configurations are neither propagated nor synced to the other node: MIPs, SNIPs, VLANs, routes (except LLB routes), route monitors, RNAT rules (except any RNAT rule with a VIP as the NAT IP), and dynamic routing configurations. They are maintained independently on each node. Default value: DISABLED Possible values = ENABLED, DISABLED
rpcnodepassword	<String>	Read-write	Password to be used in authentication with the peer rpc node.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum length = 1
hastatus	<String>	Read-write	The HA status of the node. The HA status STAYSECONDARY is used to force the secondary device stay as secondary independent of the state of the Primary device. For example, in an existing HA setup, the Primary node has to be upgraded and this process would take few seconds. During the upgradation, it is possible that the Primary node may suffer from a downtime for a few seconds. However, the Secondary should not take over as the Primary node. Thus, the Secondary node should remain as Secondary even if there is a failure in the Primary node. STAYPRIMARY configuration keeps the node in primary state in case if it is healthy, even if the peer node was the primary node initially. If the node with

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			STAYPRIMARY setting (and no peer node) is added to a primary node (which has this node as the peer) then this node takes over as the new primary and the older node becomes secondary. ENABLED state means normal HA operation without any constraints/ preferences. DISABLED state disables the normal HA operation of the node. Possible values = ENABLED, STAYSECONDARY, DISABLED, STAYPRIMARY
hasync	<String>	Read-write	Automatically maintain synchronization by duplicating the configuration of the primary node on the secondary node. This setting is not propagated. Automatic synchronization

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			requires that this setting be enabled (the default) on the current secondary node. Synchronization uses TCP port 3010. Default value: ENABLED Possible values = ENABLED, DISABLED
haprop	<String>	Read-write	Automatically propagate all commands from the primary to the secondary node, except the following: * All HA configuration related commands. For example, add ha node, set ha node, and bind ha node. * All Interface related commands. For example, set interface and unset interface. * All channels related commands. For example, add channel, set

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			channel, and bind channel. The propagated command is executed on the secondary node before it is executed on the primary. If command propagation fails, or if command execution fails on the secondary, the primary node executes the command and logs an error. Command propagation uses port 3010. Note: After enabling propagation, run force synchronization on either node. Default value: ENABLED Possible values = ENABLED, DISABLED
hellointerval	<Integer>	Read-write	Interval, in milliseconds, between heartbeat messages sent to

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			the peer node. The heartbeat messages are UDP packets sent to port 3003 of the peer node. Default value: 200 Minimum value = 200 Maximum value = 1000
deadinterval	<Integer>	Read-write	Number of seconds after which a peer node is marked DOWN if heartbeat messages are not received from the peer node. Default value: 3 Minimum value = 3 Maximum value = 60
failsafe	<String>	Read-write	Keep one node primary if both nodes fail the health check, so that a partially available node can back up data and handle traffic. This mode is set independently on each node. Default value: OFF Possible values = ON, OFF

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
maxflips	<Integer>	Read-write	Max number of flips allowed before becoming sticky primary. Default value: 0
maxfliptime	<Integer>	Read-write	Interval after which flipping of node states can again start. Default value: 0
syncvlan	<Integer>	Read-write	Vlan on which HA related communication is sent. This include sync, propagation , connection mirroring , LB persistency config sync, persistent session sync and session state sync. However HA heartbeats can go all interfaces. Minimum value = 1 Maximum value = 4094
syncstatusstrictmode	<String>	Read-write	strict mode flag for sync status. Default value: DISABLED Possible values = ENABLED, DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-only	Node Name.
flags	<Integer>	Read-only	The flags for this entry.
state	<String>	Read-only	HA Master State. Possible values = Primary, Secondary, UNKNOWN
enaifaces	<String>	Read-only	Enabled interfaces.
disifaces	<String>	Read-only	Disabled interfaces.
hamonifaces	<String>	Read-only	HAMON ON interfaces.
haheartbeatifaces	<String>	Read-only	HAHEARTBEAT OFF interfaces.
pfifaces	<String>	Read-only	Interfaces causing Partial Failure.
ifaces	<String>	Read-only	Interfaces on which non-multicast is not seen.
netmask	<String>	Read-only	The netmask.
ssl2	<String>	Read-only	SSL card status. Possible values = DOWN, UP, NOT PRESENT, UNKNOWN
masterstatetime	<Integer>	Read-only	Time elapsed in current master state.
routemonitor	<String>	Read-only	The IP address (IPv4 or IPv6).

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
curflips	<Integer>	Read-only	Keeps track of number of flips that have happened till now in current interval.
completedfliptime	<Integer>	Read-only	To inform user whether flip time is elapsed or not.
routemonitorstate	<String>	Read-only	State for route monitor. Possible values = UP, DOWN
hasyncfailurereason	<String>	Read-only	Displays the reason for HA SYNC Failure. Possible values =
secureheartbeatstate	<String>	Read-only	Displays the current state of HA secure heartbeats. Possible values = ENABLED, DISABLED
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)

- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/hanode **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"hanode":{

<b>"id":<Integer_value>,

</b><b>"ipaddress":<String_value>,

</b>"inc":<String_value>,

"rpcnodepassword":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/hanode/ id_value<Integer> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/hanode **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"hanode":{

"id":<Integer_value>,

"hastatus":<String_value>,

"hasync":<String_value>,

"haprop":<String_value>,

"hellointerval":<Integer_value>,

"deadinterval":<Integer_value>,

"failsafe":<String_value>,

"maxflips":<Integer_value>,

"maxfliptime":<Integer_value>,

"syncvlan":<Integer_value>,

"syncstatusstrictmode":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/hanode? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"hanode":{

"id":<Integer_value>,

"hastatus":true,

"hasync":true,

"haprop":true,

"hellointerval":true,

"deadinterval":true,

"failsafe":true,

"maxflips":true,

"maxfliptime":true,

"syncvlan":true,

"syncstatusstrictmode":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/hanode **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/hanode? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/hanode? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of hanode resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/hanode? **view=summary**

Use this query-parameter to get the summary output of hanode resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/hanode? **pagesize=#no;pageno=#no**

Use this query-parameter to get the hanode resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "hanode": [ {

"id":<Integer_value>,

"name":<String_value>,

"ipaddress":<String_value>,

"flags":<Integer_value>,

"hastatus":<String_value>,

"state":<String_value>,

"hasync":<String_value>,
```

```
"haprop":<String_value>,

"enaifaces":<String_value>,

"disifaces":<String_value>,

"hamonifaces":<String_value>,

"haheartbeatifaces":<String_value>,

"pfifaces":<String_value>,

"ifaces":<String_value>,

"netmask":<String_value>,

"inc":<String_value>,

"ssl2":<String_value>,

"hellointerval":<Integer_value>,

"deadinterval":<Integer_value>,

"masterstatetime":<Integer_value>,

"failsafe":<String_value>,

"routemonitor":<String_value>,

"maxflips":<Integer_value>,

"maxfliptime":<Integer_value>,

"curflips":<Integer_value>,

"completedfliptime":<Integer_value>,

"syncvlan":<Integer_value>,

"routemonitorstate":<String_value>,

"hasyncfailurereason":<String_value>,
```

```
"syncstatusstrictmode":<String_value>,

"secureheartbeatstate":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/hanode/ id_value<Integer> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/hanode/ id_value<Integer> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/hanode/ id_value<Integer> ? **view=summary**

Use this query-parameter to get the summary output of hanode resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "hanode": [ {

"id":<Integer_value>,

"name":<String_value>,

"ipaddress":<String_value>,

"flags":<Integer_value>,

"hastatus":<String_value>,

"state":<String_value>,

"hasync":<String_value>,

"haprop":<String_value>,

"enaifaces":<String_value>,

"disifaces":<String_value>,

"hamonifaces":<String_value>,

"haheartbeatifaces":<String_value>,

"pfifaces":<String_value>,

"ifaces":<String_value>,

"netmask":<String_value>,

"inc":<String_value>,

"ssl2":<String_value>,

"hellointerval":<Integer_value>,

"deadinterval":<Integer_value>,

"masterstatetime":<Integer_value>,

"failsafe":<String_value>,
```

```
"routemonitor":<String_value>,

"maxflips":<Integer_value>,

"maxfliptime":<Integer_value>,

"curflips":<Integer_value>,

"completedfliptime":<Integer_value>,

"syncvlan":<Integer_value>,

"routemonitorstate":<String_value>,

"hasyncfailurereason":<String_value>,

"syncstatusstrictmode":<String_value>,

"secureheartbeatstate":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/hanode? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "hanode": [ { "__count": "#no"} ] }
```

hanode_binding

Binding object which returns the resources bound to hanode.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
id	<Integer>	Read-write	ID of the node whose HA settings you want to display. (The ID of the local node is always 0.). Minimum value = 0 Maximum value = 64
hanode_partialfailure interfaces_binding	<hanode_partialfailur einterfaces_binding[] >	Read-only	partialfailureinterface s that can be bound to hanode.
hanode_ci_binding	<hanode_ci_binding[ ]>	Read-only	ci that can be bound to hanode.
hanode_routemonito r6_binding	<hanode_routemonit or6_binding[]>	Read-only	routemonitor6 that can be bound to hanode.
hanode_fis_binding	<hanode_fis_binding []>	Read-only	fis that can be bound to hanode.
hanode_routemonito r_binding	<hanode_routemonit or_binding[]>	Read-only	routemonitor that can be bound to hanode.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/hanode_binding/ id_value<Integer> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "hanode_binding": [ {

"id":<Integer_value>,

"hanode_routemonitor6_binding":<hanode_routemonitor6_binding[]_value>,

"hanode_partialfailureinterfaces_binding":<hanode_partialfailureinterfaces
_binding[]_value>,

"hanode_fis_binding":<hanode_fis_binding[]_value>,

"hanode_ci_binding":<hanode_ci_binding[]_value>,

"hanode_routemonitor_binding":<hanode_routemonitor_binding[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/hanode_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/hanode_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "hanode_binding": [ {

"id":<Integer_value>,

"hanode_routemonitor6_binding":<hanode_routemonitor6_binding[]_value>,

"hanode_partialfailureinterfaces_binding":<hanode_partialfailureinterfaces
_binding[]_value>,

"hanode_fis_binding":<hanode_fis_binding[]_value>,

"hanode_ci_binding":<hanode_ci_binding[]_value>,

"hanode_routemonitor_binding":<hanode_routemonitor_binding[]_value>

}]}
```

hanode_ci_binding

Binding object showing the ci that can be bound to hanode.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
routemonitor	<String>	Read-write	A route that you want the Citrix ADC to monitor in its internal routing table. You can specify an IPv4

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			address or network, or an IPv6 address or network prefix. If you specify an IPv4 network address or IPv6 network prefix, the appliance monitors any route that matches the network or prefix. Minimum length = 1
id	<Integer>	Read-write	Number that uniquely identifies the local node. The ID of the local node is always 0. Minimum value = 0 Maximum value = 64
enaifaces	<String>	Read-write	Enabled interfaces.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/hanode_ci_binding/ id_value<Integer> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/hanode_ci_binding/ id_value<Integer> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of hanode_ci_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/hanode_ci_binding/ id_value<Integer> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the hanode_ci_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "hanode_ci_binding": [ {

"routemonitor":<String_value>,

"id":<Integer_value>,

"enaifaces":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/hanode_ci_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/hanode_ci_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "hanode_ci_binding": [ {

"routemonitor":<String_value>,

"id":<Integer_value>,

"enaifaces":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/hanode_ci_binding/ id_value<Integer> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"hanode_ci_binding": [ { "__count": "#no"} ] }
```

hanode_fis_binding

Binding object showing the fis that can be bound to hanode.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Node Name.
id	<Integer>	Read-write	Number that uniquely identifies the local node. The ID of the local node is always 0. Minimum value = 0 Maximum value = 64
routemonitor	<String>	Read-write	A route that you want the Citrix ADC to monitor in its internal routing table. You can specify an IPv4 address or network, or an IPv6 address or network prefix. If you specify an IPv4 network address or IPv6 network prefix, the appliance monitors any route that matches the network or prefix. Minimum length = 1
enaifaces	<String>	Read-only	Enabled interfaces.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/hanode_fis_binding/ id_value<Integer> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/hanode_fis_binding/ id_value<Integer> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of hanode_fis_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/hanode_fis_binding/ id_value<Integer> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the hanode_fis_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "hanode_fis_binding": [ {

"name":<String_value>,

"id":<Integer_value>,

"routemonitor":<String_value>,

"enaifaces":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/hanode_fis_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/hanode_fis_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "hanode_fis_binding": [ {

"name":<String_value>,

"id":<Integer_value>,

"routemonitor":<String_value>,

"enaifaces":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/hanode_fis_binding/ id_value<Integer> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"hanode_fis_binding": [ { "__count": "#no"} ] }
```

hanode_partialfailureinterfaces_binding

Binding object showing the partialfailureinterfaces that can be bound to hanode.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
pfifaces	<String>	Read-write	Interfaces causing Partial Failure.
id	<Integer>	Read-write	Number that uniquely identifies the local node. The ID of the local node is always 0. Minimum value = 0 Maximum value = 64
routemonitor	<String>	Read-write	A route that you want the Citrix ADC to monitor in its internal routing table. You can specify an IPv4 address or network, or an IPv6 address or network prefix. If you specify an IPv4 network address or IPv6 network prefix, the appliance monitors any route that matches the network or prefix. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/hanode_partialfailureinterfaces_binding/ id_value<Integer> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ hanode_partialfailureinterfaces_binding/ id_value<Integer> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of hanode_partialfailureinterfaces_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/hanode_partialfailureinterfaces_binding/ id_value<Integer> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the hanode_partialfailureinterfaces_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "hanode_partialfailureinterfaces_binding": [ {

"pfifaces":<String_value>,

"id":<Integer_value>,

"routemonitor":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/hanode_partialfailureinterfaces_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/hanode_partialfailureinterfaces_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "hanode_partialfailureinterfaces_binding": [ {

"pfifaces":<String_value>,

"id":<Integer_value>,

"routemonitor":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/hanode_partialfailureinterfaces_binding/id_value<Integer> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"hanode_partialfailureinterfaces_binding": [ { "__count": "#no"} ] }
```

hanode_routemonitor6_binding

Binding object showing the routemonitor6 that can be bound to hanode.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
netmask	<String>	Read-write	The netmask.
routemonitor	<String>	Read-write	The IP address (IPv4 or IPv6).
id	<Integer>	Read-write	Number that uniquely identifies the local node. The ID of the local node is always 0. Minimum value = 0 Maximum value = 64

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
flags	<Integer>	Read-only	The flags for this entry.
routemonitorstate	<String>	Read-only	State for route monitor. Possible values = UP, DOWN
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/hanode_routemonitor6_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"hanode_routemonitor6_binding":{

"id":<Integer_value>,

<b>"routemonitor":<String_value>,

</b>"netmask":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/hanode_routemonitor6_binding/ id_value<Integer> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ hanode_routemonitor6_binding/ id_value<Integer> ? **args= routemonitor:<String_value>, netmask: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/hanode_routemonitor6_binding/ id_value<Integer> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ hanode_routemonitor6_binding/ id_value<Integer> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of hanode_routemonitor6_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/hanode_routemonitor6_binding/ id_value<Integer> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the hanode_routemonitor6_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "hanode_routemonitor6_binding": [ {

"netmask":<String_value>,

"routemonitor":<String_value>,

"id":<Integer_value>,

"flags":<Integer_value>,

"routemonitorstate":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/hanode_routemonitor6_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/hanode_routemonitor6_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "hanode_routemonitor6_binding": [ {

"netmask":<String_value>,

"routemonitor":<String_value>,

"id":<Integer_value>,

"flags":<Integer_value>,

"routemonitorstate":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/hanode_routemonitor6_binding/ id_value<Integer> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"hanode_routemonitor6_binding": [ { "__count": "#no"} ] }
```

hanode_routemonitor_binding

Binding object showing the routemonitor that can be bound to hanode.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
netmask	<String>	Read-write	The netmask.
id	<Integer>	Read-write	Number that uniquely identifies the local node. The ID of the local node is always 0. Minimum value = 0 Maximum value = 64
routemonitor	<String>	Read-write	The IP address (IPv4 or IPv6).
routemonitorstate	<String>	Read-only	State for route monitor. Possible values = UP, DOWN
flags	<Integer>	Read-only	The flags for this entry.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/hanode_routemonitor_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"hanode_routemonitor_binding":{

"id":<Integer_value>,
```

```
<b>"routemonitor":<String_value>,

</b>"netmask":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/hanode_routemonitor_binding/ id_value<Integer> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ hanode_routemonitor_binding/ id_value<Integer> ? **args= routemonitor:<String_value>, netmask: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/hanode_routemonitor_binding/ id_value<Integer> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ hanode_routemonitor_binding/ id_value<Integer> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of hanode_routemonitor_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/hanode_routemonitor_binding/ id_value<Integer> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the hanode_routemonitor_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "hanode_routemonitor_binding": [ {

"netmask":<String_value>,

"id":<Integer_value>,

"routemonitor":<String_value>,

"routemonitorstate":<String_value>,

"flags":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/hanode_routemonitor_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/hanode_routemonitor_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "hanode_routemonitor_binding": [ {

"netmask":<String_value>,

"id":<Integer_value>,

"routemonitor":<String_value>,

"routemonitorstate":<String_value>,

"flags":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/hanode_routemonitor_binding/id_value<Integer> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"hanode_routemonitor_binding": [ { "__count": "#no"} ] }
```

hasync

Configuration for sync resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
force	<Boolean>	Read-write	Force synchronization regardless of the state of HA propagation and HA synchronization on either node.
save	<String>	Read-write	After synchronization, automatically save the configuration in the secondary node configuration file (ns.conf) without prompting for confirmation. Possible values = YES, NO

Operations

(click to see Properties)

- FORCE

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

FORCE

URL: http:// <netscaler-ip-address> /nitro/v1/config/hasync? **action=Force HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"hasync":{

"force":<Boolean_value>,

"save":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

hasyncfailures

Configuration for HA sync failures resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
response	<String>	Read-write	Displays the list of commands failed during HA configuration synchronization.
_nextgenapiresource	<String>	Read-write	.

Operations

(click to see Properties)

- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/hasyncfailures

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "hasyncfailures": [ {

"response":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

ica

Ica

ICA configuration.

NAME	DESCRIPTION
icaaccessprofile	Configuration for ica accessprofile
icaaction	Configuration for ica action
icaglobal_binding	Binding object showing the resources that can be bound to icaglobal
icaglobal_icapolicy_binding	Binding object showing the icapolicy that can be bound to icaglobal
icalatencyprofile	Configuration for Profile for Latency monitoring
icaparameter	Configuration for Config Parameters for NS ICA
icapolicy	Configuration for ICA policy

NAME	DESCRIPTION
icapolicy_binding	Binding object showing the resources that can be bound to icapolicy
icapolicy_crvserver_binding	Binding object showing the crvserver that can be bound to icapolicy
icapolicy_icaglobal_binding	Binding object showing the icaglobal that can be bound to icapolicy
icapolicy_vpnvserver_binding	Binding object showing the vpnvserver that can be bound to icapolicy

icaaccessprofile

Configuration for ica accessprofile resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the ICA accessprofile. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			the ICA accessprofile is added. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my ica accessprofile" or 'my ica accessprofile'). Each of the features can be configured as DEFAULT/ DISABLED. Here, DISABLED means that the policy settings on the backend XenApp/ XenDesktop server are overridden and the Citrix ADC makes the decision to deny access. Whereas DEFAULT means that the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Citrix ADC allows the request to reach the XenApp/ XenDesktop that takes the decision to allow/deny access based on the policy configured on it. For example, if ClientAudioRedirect ion is enabled on the backend XenApp/ XenDesktop server, and the configured profile has ClientAudioRedirect ion as DISABLED, the Citrix ADC makes the decision to deny the request irrespective of the configuration on the backend. If the configured profile has ClientAudioRedirect ion as DEFAULT, then the Citrix ADC forwards the requests to the backend XenApp/ XenDesktop server.It then makes the decision to

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			allow/deny access based on the policy configured on it. Minimum length = 1
connectclientlptports	<String>	Read-write	Allow Default access/Disable automatic connection of LPT ports from the client when the user logs on. Default value: DISABLED Possible values = DEFAULT, DISABLED
clientaudioredirection	<String>	Read-write	Allow Default access/Disable applications hosted on the server to play sounds through a sound device installed on the client computer, also allows or prevents users to record audio input. Default value: DISABLED Possible values = DEFAULT, DISABLED
localremotedatasharing	<String>	Read-write	Allow Default access/Disable file/

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			data sharing via the Receiver for HTML5. Default value: DISABLED Possible values = DEFAULT, DISABLED
clientclipboardredirection	<String>	Read-write	Allow Default access/Disable the clipboard on the client device to be mapped to the clipboard on the server. Default value: DISABLED Possible values = DEFAULT, DISABLED
clientcomportredirection	<String>	Read-write	Allow Default access/Disable COM port redirection to and from the client. Default value: DISABLED Possible values = DEFAULT, DISABLED
clientdriveredirection	<String>	Read-write	Allow Default access/Disables drive redirection to and from the client.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: DISABLED Possible values = DEFAULT, DISABLED
clientprinterredirection	<String>	Read-write	Allow Default access/Disable client printers to be mapped to a server when a user logs on to a session. Default value: DISABLED Possible values = DEFAULT, DISABLED
multistream	<String>	Read-write	Allow Default access/Disable the multistream feature for the specified users. Default value: DISABLED Possible values = DEFAULT, DISABLED
clientusbdriveredirection	<String>	Read-write	Allow Default access/Disable the redirection of USB devices to and from the client. Default value: DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = DEFAULT, DISABLED
clienttwaindeviceredirection	<String>	Read-write	Allow default access or disable TWAIN devices, such as digital cameras or scanners, on the client device from published image processing applications. Default value: DISABLED Possible values = DEFAULT, DISABLED
wiaredirection	<String>	Read-write	Allow default access or disable WIA scanner redirection. Default value: DISABLED Possible values = DEFAULT, DISABLED
draganddrop	<String>	Read-write	Allow default access or disable drag and drop between client and remote applications and desktops. Default value: DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = DEFAULT, DISABLED
smartcardredirection	<String>	Read-write	Allow default access or disable smart card redirection. Smart card virtual channel is always allowed in CVAD. Default value: DISABLED Possible values = DEFAULT, DISABLED
fido2redirection	<String>	Read-write	Allow default access or disable FIDO2 redirection. Default value: DISABLED Possible values = DEFAULT, DISABLED
refcnt	<Integer>	Read-only	Number of entities using this accessprofile.
builtin	<String[]>	Read-only	Indicates that the ICA accessprofile is a built-in (SYSTEM INTERNAL) type. Possible values = MODIFIABLE, DELETABLE,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			IMMUTABLE, PARTITION_ALL
feature	<String>	Read-only	The feature to be checked while applying this config.
isdefault	<Boolean>	Read-only	A value of true is returned if it is a default accessprofile.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/icaaccessprofile **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"icaaccessprofile":{

<b>"name":<String_value>,

</b>"connectclientlptports":<String_value>,

"clientaudioredirection":<String_value>,

"localremotedatasharing":<String_value>,

"clientclipboardredirection":<String_value>,

"clientcomportredirection":<String_value>,

"clientdriveredirection":<String_value>,
```

```
"clientprinterredirection":<String_value>,

"multistream":<String_value>,

"clientusbdriveredirection":<String_value>,

"clienttwaindeviceredirection":<String_value>,

"wiaredirection":<String_value>,

"draganddrop":<String_value>,

"smartcardredirection":<String_value>,

"fido2redirection":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/icaaccessprofile/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/icaaccessprofile **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"icaaccessprofile":{

<b>"name":<String_value>,

</b>"connectclientlptports":<String_value>,

"clientaudioredirection":<String_value>,

"localremotedatasharing":<String_value>,

"clientclipboardredirection":<String_value>,

"clientcomportredirection":<String_value>,

"clientdriveredirection":<String_value>,

"clientprinterredirection":<String_value>,

"multistream":<String_value>,

"clientusbdriveredirection":<String_value>,

"clienttwaindeviceredirection":<String_value>,

"wiaredirection":<String_value>,

"draganddrop":<String_value>,

"smartcardredirection":<String_value>,

"fido2redirection":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/icaaccessprofile? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"icaaccessprofile":{

<b>"name":<String_value>,

</b>"connectclientlptports":true,

"clientaudioredirection":true,

"localremotedatasharing":true,

"clientclipboardredirection":true,

"clientcomportredirection":true,

"clientdriveredirection":true,

"clientprinterredirection":true,

"multistream":true,

"clientusbdriveredirection":true,

"clienttwaindeviceredirection":true,

"wiaredirection":true,

"draganddrop":true,

"smartcardredirection":true,

"fido2redirection":true
```

```
}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/icaaccessprofile **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/icaaccessprofile? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/icaaccessprofile? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of icaaccessprofile resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/icaaccessprofile? **view=summary**

Use this query-parameter to get the summary output of icaaccessprofile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/icaaccessprofile? **pagesize=#no;pageno=#no**

Use this query-parameter to get the icaaccessprofile resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "icaaccessprofile": [ {

"name":<String_value>,

"connectclientlptports":<String_value>,

"clientaudioredirection":<String_value>,

"localremotedatasharing":<String_value>,

"clientclipboardredirection":<String_value>,

"clientcomportredirection":<String_value>,

"clientdriveredirection":<String_value>,

"clientprinterredirection":<String_value>,

"multistream":<String_value>,

"clientusbdriveredirection":<String_value>,

"clienttwaindeviceredirection":<String_value>,

"wiaredirection":<String_value>,

"draganddrop":<String_value>,

"smartcardredirection":<String_value>,

"fido2redirection":<String_value>,

"refcnt":<Integer_value>,
```

```
"builtin":<String[]_value>,

"feature":<String_value>,

"isdefault":<Boolean_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/icaaccessprofile/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/icaaccessprofile/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/icaaccessprofile/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of icaaccessprofile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "icaaccessprofile": [ {

"name":<String_value>,

"connectclientlptports":<String_value>,

"clientaudioredirection":<String_value>,

"localremotedatasharing":<String_value>,

"clientclipboardredirection":<String_value>,

"clientcomportredirection":<String_value>,

"clientdriveredirection":<String_value>,

"clientprinterredirection":<String_value>,

"multistream":<String_value>,

"clientusbdriveredirection":<String_value>,

"clienttwaindeviceredirection":<String_value>,

"wiaredirection":<String_value>,

"draganddrop":<String_value>,

"smartcardredirection":<String_value>,

"fido2redirection":<String_value>,

"refcnt":<Integer_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"isdefault":<Boolean_value>,

"_nextgenapiresource":<String_value>
```

```
}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/icaaccessprofile? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "icaaccessprofile": [ { "__count": "#no"} ] }
```

icaaction

Configuration for ica action resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the ICA action. Must begin with a letter, number, or the underscore character (_), and must contain only

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after the ICA action is added. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my ica action" or 'my ica action'). Minimum length = 1
accessprofilename	<String>	Read-write	Name of the ica accessprofile to be associated with this action.
latencyprofilename	<String>	Read-write	Name of the ica latencyprofile to be associated with this action.
newname	<String>	Read-write	New name for the ICA action. Must begin with an ASCII alphabetic or underscore (_)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			character, and must contain only ASCII alphanumeric, underscore, hash (#),period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my ica action" or 'my ica action'). Minimum length = 1
hits	<Integer>	Read-only	The number of times the action has been taken.
referencecount	<Integer>	Read-only	The number of references to the action.
undefhits	<Integer>	Read-only	The number of times the action resulted in UNDEF.
builtin	<String[]>	Read-only	Indicates that the ICA action is a built-

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			in (SYSTEM INTERNAL) type. Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL
feature	<String>	Read-only	The feature to be checked while applying this config.
isdefault	<Boolean>	Read-only	A value of true is returned if it is a default action.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- RENAME
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/icaaction **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"icaaction":{

<b>"name":<String_value>,

</b>"accessprofilename":<String_value>,

"latencyprofilename":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/icaaction/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/icaaction **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"icaaction":{

<b>"name":<String_value>,

</b>"accessprofilename":<String_value>,

"latencyprofilename":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/icaaction? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"icaaction":{

<b>"name":<String_value>,

</b>"accessprofilename":true,

"latencyprofilename":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

RENAME

URL: http:// <netscaler-ip-address> /nitro/v1/config/icaaction? **action=rename HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"icaaction":{

<b>"name":<String_value>,

</b><b>"newname":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/icaaction **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/icaaction? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/icaaction? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of icaaction resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/icaaction? **view=summary**

Use this query-parameter to get the summary output of icaaction resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/icaaction? **pagesize=#no;pageno=#no**

Use this query-parameter to get the icaaction resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "icaaction": [ {

"name":<String_value>,

"accessprofilename":<String_value>,

"latencyprofilename":<String_value>,

"hits":<Integer_value>,

"referencecount":<Integer_value>,

"undefhits":<Integer_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"isdefault":<Boolean_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/icaaction/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/icaaction/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/icaaction/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of icaaction resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "icaaction": [ {

"name":<String_value>,

"accessprofilename":<String_value>,

"latencyprofilename":<String_value>,

"hits":<Integer_value>,

"referencecount":<Integer_value>,

"undefhits":<Integer_value>,

"builtin":<String[]_value>,

"feature":<String_value>,
```

```
"isdefault":<Boolean_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/icaaction? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "icaaction": [ { "__count": "#no"} ] }
```

icaglobal_binding

Binding object which returns the resources bound to icaglobal.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
icaglobal_icapolicy_binding	<icaglobal_icapolicy_binding[]>	Read-write	icapolicy that can be bound to icaglobal.

Operations

(click to see Properties)

- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/icaglobal_binding

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "icaglobal_binding": [ {

"icaglobal_icapolicy_binding":<icaglobal_icapolicy_binding[]_value>

}]}
```

icaglobal_icapolicy_binding

Binding object showing the icapolicy that can be bound to icaglobal.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
priority	<Integer>	Read-write	Specifies the priority of the policy.
type	<String>	Read-write	Global bind point for which to show detailed information about the policies bound to the bind point. Possible values = ICA_REQ_OVERRIDE,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			ICA_REQ_DEFAULT
gotopriorityexpression	<String>	Read-write	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
globalbindtype	<String>	Read-write	. Default value: SYSTEM_GLOBAL Possible values = SYSTEM_GLOBAL, VPN_GLOBAL, RNAT_GLOBAL, APPFW_GLOBAL, TM_GLOBAL
policyname	<String>	Read-write	Name of the ICA policy.
flowtype	<Integer>	Read-only	Flow type of the bound ICA policy.
numpol	<Integer>	Read-only	The number of policies bound to the bindpoint.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE

- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/icaglobal_icapolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"icaglobal_icapolicy_binding":{

<b>"policyname":<String_value>,

</b><b>"priority":<Integer_value>,

</b>"gotopriorityexpression":<String_value>,

"type":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/icaglobal_icapolicy_binding **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/icaglobal_icapolicy_binding? **args= policyname:<String_value>, type: <String_value> ,priority: <Integer_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/icaglobal_icapolicy_binding **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/icaglobal_icapolicy_binding? **args=type: <String_value>**

Use this query-parameter to get icaglobal_icapolicy_binding resources based on additional properties.

filter http:// <netscaler-ip-address> /nitro/v1/config/icaglobal_icapolicy_binding? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of icaglobal_icapolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/icaglobal_icapolicy_binding? **pagesize=#no;pageno=#no**

Use this query-parameter to get the icaglobal_icapolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "icaglobal_icapolicy_binding": [ {

"priority":<Integer_value>,

"type":<String_value>,

"gotopriorityexpression":<String_value>,

"globalbindtype":<String_value>,

"policyname":<String_value>,

"flowtype":<Integer_value>,
```

```
"numpol":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/icaglobal_icapolicy_binding? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "icaglobal_icapolicy_binding": [ { "__count": "#no"} ] }
```

icalatencyprofile

Configuration for Profile for Latency monitoring resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the ICA latencyprofile. Must begin with a letter, number, or the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after the ICA latency profile is added. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my ica l7latencyprofile" or 'my ica l7latencyprofile'). Minimum length = 1
l7latencymonitoring	<String>	Read-write	Enable/Disable L7 Latency monitoring for L7 latency notifications.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: DISABLED Possible values = ENABLED, DISABLED
l7latencythresholdfactor	<Integer>	Read-write	L7 Latency threshold factor. This is the factor by which the active latency should be greater than the minimum observed value to determine that the latency is high and may need to be reported. Default value: 4 Minimum value = 2 Maximum value = 65535
l7latencywaittime	<Integer>	Read-write	L7 Latency Wait time. This is the time for which the Citrix ADC waits after the threshold is exceeded before it sends out a Notification to the Insight Center. Default value: 20 Minimum value = 1 Maximum value = 65535

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
l7latencynotifyinterval	<Integer>	Read-write	L7 Latency Notify Interval. This is the interval at which the Citrix ADC sends out notifications to the Insight Center after the wait time has passed. Default value: 20 Minimum value = 1 Maximum value = 65535
l7latencymaxnotifycount	<Integer>	Read-write	L7 Latency Max notify Count. This is the upper limit on the number of notifications sent to the Insight Center within an interval where the Latency is above the threshold. Default value: 5 Minimum value = 1 Maximum value = 65535
refcnt	<Integer>	Read-only	Number of entities using this l7latencyprofile.
builtin	<String[]>	Read-only	Indicates that the ICA latencyprofile is a built-in (SYSTEM INTERNAL) type.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL
feature	<String>	Read-only	The feature to be checked while applying this config.
isdefault	<Boolean>	Read-only	A value of true is returned if it is a default l7latencyprofile.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/icalatencyprofile **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"icalatencyprofile":{

<b>"name":<String_value>,

</b>"l7latencymonitoring":<String_value>,

"l7latencythresholdfactor":<Integer_value>,

"l7latencywaittime":<Integer_value>,

"l7latencynotifyinterval":<Integer_value>,

"l7latencymaxnotifycount":<Integer_value>
```

```
}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/icalatencyprofile/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/icalatencyprofile **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"icalatencyprofile":{

<b>"name":<String_value>,

</b>"l7latencymonitoring":<String_value>,

"l7latencythresholdfactor":<Integer_value>,

"l7latencywaittime":<Integer_value>,

"l7latencynotifyinterval":<Integer_value>,
```

```
"l7latencymaxnotifycount":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/icalatencyprofile? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"icalatencyprofile":{

<b>"name":<String_value>,

</b>"l7latencymonitoring":true,

"l7latencythresholdfactor":true,

"l7latencywaittime":true,

"l7latencynotifyinterval":true,

"l7latencymaxnotifycount":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/icalatencyprofile **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/icalatencyprofile? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/icalatencyprofile? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of icalatencyprofile resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/icalatencyprofile? **view=summary**

Use this query-parameter to get the summary output of icalatencyprofile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/icalatencyprofile? **pagesize=#no;pageno=#no**

Use this query-parameter to get the icalatencyprofile resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "icalatencyprofile": [ {

"name":<String_value>,

"l7latencymonitoring":<String_value>,

"l7latencythresholdfactor":<Integer_value>,

"l7latencywaittime":<Integer_value>,

"l7latencynotifyinterval":<Integer_value>,

"l7latencymaxnotifycount":<Integer_value>,

"refcnt":<Integer_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"isdefault":<Boolean_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/icalatencyprofile/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/icalatencyprofile/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/icalatencyprofile/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of icalatencyprofile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "icalatencyprofile": [ {

"name":<String_value>,

"l7latencymonitoring":<String_value>,

"l7latencythresholdfactor":<Integer_value>,

"l7latencywaittime":<Integer_value>,

"l7latencynotifyinterval":<Integer_value>,

"l7latencymaxnotifycount":<Integer_value>,

"refcnt":<Integer_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"isdefault":<Boolean_value>,

"_nextgenapiresource":<String_value>
```

```
}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/icalatencyprofile? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "icalatencyprofile": [ { "__count": "#no"} ] }
```

icaparameter

Configuration for Config Parameters for NS ICA resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
enablesronhafailover	<String>	Read-write	Enable/Disable Session Reliability on HA failover. The default value is No. Default value: NO

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = YES, NO
hdxinsightnonnsap	<String>	Read-write	Enable/Disable HDXInsight for Non NSAP ICA Sessions. The default value is Yes. Default value: YES Possible values = YES, NO
edtpmtuddf	<String>	Read-write	Enable/Disable DF enforcement for EDT PMTUD Control Blocks. Default value: ENABLED Possible values = ENABLED, DISABLED
edtpmtuddftimeout	<Integer>	Read-write	DF enforcement timeout for EDTPMTUDDF. Default value: 100 Minimum value = 10 Maximum value = 65535
l7latencyfrequency	<Integer>	Read-write	Specify the time interval/period for which L7 Client Latency value is to be calculated. By default, L7 Client Latency is calculated

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			for every packet. The default value is 0. Default value: 0 Minimum value = 0 Maximum value = 60
edtlosstolerant	<String>	Read-write	Enable/Disable EDT Loss Tolerant feature. Default value: DISABLED Possible values = ENABLED, DISABLED
edtpmtudrediscovery	<String>	Read-write	Enable/Disable EDT PMTUD Rediscovery. Default value: DISABLED Possible values = ENABLED, DISABLED
dfpersistence	<String>	Read-write	Enable/Disable DF Persistence. Default value: DISABLED Possible values = ENABLED, DISABLED
insightonlytodirector	<String>	Read-write	Enable/Disable HDX Insight data to

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Director even if HDX Insight policy is not configured on Gateway and Network Telemtry policy is enabled on VDA. Default value: ENABLED Possible values = ENABLED, DISABLED
builtin	<String[]>	Read-only	Indicates that the ICA parameter is a built-in (SYSTEM INTERNAL) type. Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- UPDATE
- UNSET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/icaparameter **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"icaparameter":{

"enablesronhafailover":<String_value>,

"hdxinsightnonnsap":<String_value>,

"edtpmtuddf":<String_value>,

"edtpmtuddftimeout":<Integer_value>,

"l7latencyfrequency":<Integer_value>,
```

```
"edtlosstolerant":<String_value>,

"edtpmtudrediscovery":<String_value>,

"dfpersistence":<String_value>,

"insightonlytodirector":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/icaparameter? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"icaparameter":{

"enablesronhafailover":true,

"hdxinsightnonnsap":true,

"edtpmtuddf":true,

"edtpmtuddftimeout":true,

"l7latencyfrequency":true,

"edtlosstolerant":true,
```

```
"edtpmtudrediscovery":true,

"dfpersistence":true,

"insightonlytodirector":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/icaparameter **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "icaparameter": [ {

"enablesronhafailover":<String_value>,

"hdxinsightnonnsap":<String_value>,

"edtpmtuddf":<String_value>,

"edtpmtuddftimeout":<Integer_value>,
```

```
"builtin":<String[]_value>,

"l7latencyfrequency":<Integer_value>,

"edtlosstolerant":<String_value>,

"edtpmtudrediscovery":<String_value>,

"dfpersistence":<String_value>,

"insightonlytodirector":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

icapolicy

Configuration for ICA policy resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the policy. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. The following requirement applies

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my ica policy" or 'my ica policy').
rule	<String>	Read-write	Expression or other value against which the traffic is evaluated. Must be a Boolean expression. The following requirements apply only to the Citrix ADC CLI: * If the expression includes one or more spaces, enclose the entire expression in double quotation marks. * If the expression itself includes double quotation marks, escape the quotations by using the \ character.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			* Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks.
action	<String>	Read-write	Name of the ica action to be associated with this policy.
comment	<String>	Read-write	Any type of information about this ICA policy.
logaction	<String>	Read-write	Name of the messagelog action to use for requests that match this policy.
newname	<String>	Read-write	New name for the policy. Must begin with an ASCII alphabetic or underscore (_)character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), s pace, colon (:), at (@), equals (=), and hyphen (-) characters.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my ica policy" or 'my ica policy'). Minimum length = 1
hits	<Integer>	Read-only	Number of hits.
undefhits	<Integer>	Read-only	Number of policy UNDEF hits.
builtin	<String[]>	Read-only	Indicates that the ICA policy is a built-in (SYSTEM INTERNAL) type. Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL
feature	<String>	Read-only	The feature to be checked while applying this config.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- RENAME
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/icapolicy **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"icapolicy":{

<b>"name":<String_value>,

</b><b>"rule":<String_value>,

</b><b>"action":<String_value>,

</b>"comment":<String_value>,

"logaction":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/icapolicy/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/icapolicy **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"icapolicy":{

<b>"name":<String_value>,

</b>"rule":<String_value>,

"action":<String_value>,

"comment":<String_value>,

"logaction":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/icapolicy? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"icapolicy":{

<b>"name":<String_value>,

</b>"comment":true,

"logaction":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

RENAME

URL: http:// <netscaler-ip-address> /nitro/v1/config/icapolicy? **action=rename HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"icapolicy":{

<b>"name":<String_value>,

</b><b>"newname":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/icapolicy **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/icapolicy? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/icapolicy? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of icapolicy resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/icapolicy? **view=summary**

Use this query-parameter to get the summary output of icapolicy resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/icapolicy? **pagesize=#no;pageno=#no**

Use this query-parameter to get the icapolicy resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "icapolicy": [ {

"name":<String_value>,
```

```
"rule":<String_value>,

"action":<String_value>,

"hits":<Integer_value>,

"undefhits":<Integer_value>,

"comment":<String_value>,

"logaction":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/icapolicy/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/icapolicy/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/icapolicy/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of icapolicy resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "icapolicy": [ {

"name":<String_value>,

"rule":<String_value>,

"action":<String_value>,

"hits":<Integer_value>,

"undefhits":<Integer_value>,

"comment":<String_value>,

"logaction":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/icapolicy? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "icapolicy": [ { "__count": "#no"} ] }
```

icapolicy_binding

Binding object which returns the resources bound to icapolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the policy about which to display detailed information.
icapolicy_crvserver_binding	<icapolicy_crvserver_binding[]>	Read-only	crvserver that can be bound to icapolicy.
icapolicy_icaglobal_binding	<icapolicy_icaglobal_binding[]>	Read-only	icaglobal that can be bound to icapolicy.
icapolicy_vpnvserver_binding	<icapolicy_vpnvserver_binding[]>	Read-only	vpnvserver that can be bound to icapolicy.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/icapolicy_binding/ name_value<String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "icapolicy_binding": [ {

"name":<String_value>,

"icapolicy_crvserver_binding":<icapolicy_crvserver_binding[]_value>,

"icapolicy_icaglobal_binding":<icapolicy_icaglobal_binding[]_value>,

"icapolicy_vpnvserver_binding":<icapolicy_vpnvserver_binding[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/icapolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/icapolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "icapolicy_binding": [ {

"name":<String_value>,

"icapolicy_crvserver_binding":<icapolicy_crvserver_binding[]_value>,

"icapolicy_icaglobal_binding":<icapolicy_icaglobal_binding[]_value>,

"icapolicy_vpnvserver_binding":<icapolicy_vpnvserver_binding[]_value>

}]}
```

icapolicy_crvserver_binding

Binding object showing the crvserver that can be bound to icapolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
boundto	<String>	Read-write	Location where policy is bound.
name	<String>	Read-write	Name of the policy about which to display detailed information.
activepolicy	<Integer>	Read-only	Indicates whether policy is bound or not.
gotopriorityexpression	<String>	Read-only	Expression specifying the priority of the next policy which will get evaluated if the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			current policy rule evaluates to TRUE.
priority	<Integer>	Read-only	Specifies the priority of the policy.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/icapolicy_crvserver_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ icapolicy_crvserver_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of icapolicy_crvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/icapolicy_crvserver_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the icapolicy_crvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "icapolicy_crvserver_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"activepolicy":<Integer_value>,

"gotopriorityexpression":<String_value>,
```

```
"priority":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/icapolicy_crvserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/icapolicy_crvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "icapolicy_crvserver_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"activepolicy":<Integer_value>,

"gotopriorityexpression":<String_value>,
```

```
"priority":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/icapolicy_crvserver_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"icapolicy_crvserver_binding": [ { "__count": "#no"} ] }
```

icapolicy_icaglobal_binding

Binding object showing the icaglobal that can be bound to icapolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the policy about which to display detailed information.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
boundto	<String>	Read-write	Location where policy is bound.
priority	<Integer>	Read-only	Specifies the priority of the policy.
activepolicy	<Integer>	Read-only	Indicates whether policy is bound or not.
gotopriorityexpression	<String>	Read-only	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of

creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/icapolicy_icaglobal_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ icapolicy_icaglobal_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of icapolicy_icaglobal_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/icapolicy_icaglobal_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the icapolicy_icaglobal_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "icapolicy_icaglobal_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"priority":<Integer_value>,

"activepolicy":<Integer_value>,

"gotopriorityexpression":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/icapolicy_icaglobal_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/icapolicy_icaglobal_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "icapolicy_icaglobal_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"priority":<Integer_value>,

"activepolicy":<Integer_value>,

"gotopriorityexpression":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/icapolicy_icaglobal_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"icapolicy_icaglobal_binding": [ { "__count": "#no"} ] }
```

icapolicy_vpnvserver_binding

Binding object showing the vpnvserver that can be bound to icapolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the policy about which to display detailed information.
boundto	<String>	Read-write	Location where policy is bound.
gotopriorityexpression	<String>	Read-only	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
activepolicy	<Integer>	Read-only	Indicates whether policy is bound or not.
priority	<Integer>	Read-only	Specifies the priority of the policy.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/icapolicy_vpnvserver_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ icapolicy_vpnvserver_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of icapolicy_vpnvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/icapolicy_vpnvserver_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the icapolicy_vpnvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "icapolicy_vpnvserver_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"gotopriorityexpression":<String_value>,

"activepolicy":<Integer_value>,

"priority":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/icapolicy_vpnvserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/icapolicy_vpnvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "icapolicy_vpnvserver_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"gotopriorityexpression":<String_value>,

"activepolicy":<Integer_value>,

"priority":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/icapolicy_vpnvserver_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"icapolicy_vpnvserver_binding": [ { "__count": "#no"} ] }
```

ipsec

Ipsec

IPSEC configuration.

NAME	DESCRIPTION
ipsecparameter	Configuration for IPSEC paramter
ipsecprofile	Configuration for IPSEC profile

ipsecparameter

Configuration for IPSEC paramter resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ikeversion	<String>	Read-write	IKE Protocol Version. Default value: V2 Possible values = V1, V2
encalgo	<String[]>	Read-write	Type of encryption algorithm (Note: Selection of AES enables AES128). Default value: AES

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = AES, AES192, AES256
hashalgo	<String[]>	Read-write	Type of hashing algorithm. Default value: HMAC_SHA256 Possible values = HMAC_SHA1, HMAC_SHA256, HMAC_SHA384, HMAC_SHA512, HMAC_MD5
lifetime	<Integer>	Read-write	Lifetime of IKE SA in seconds. Lifetime of IPSec SA will be (lifetime of IKE SA/ 8). Minimum value = 480 Maximum value = 31536000
livenesscheckinterval	<Integer>	Read-write	Number of seconds after which a notify payload is sent to check the liveliness of the peer. Additional retries are done as per retransmit interval setting. Zero value disables liveliness checks. Minimum value = 0

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum value = 64999
replaywindowsize	<Integer>	Read-write	IPSec Replay window size for the data traffic. Minimum value = 0 Maximum value = 16384
ikeretryinterval	<Integer>	Read-write	IKE retry interval for bringing up the connection. Minimum value = 60 Maximum value = 3600
perfectforwardsecrecy	<String>	Read-write	Enable/Disable PFS. Default value: DISABLE Possible values = ENABLE, DISABLE
retransmissiontime	<Integer>	Read-write	The interval in seconds to retry sending the IKE messages to peer, three consecutive attempts are done with doubled interval after every failure, increases for every retransmit till 6 retransmits. Minimum value = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum value = 99
responderonly	<String>	Read-only	Responder Only config for IKED. Default value: NO Possible values = YES, NO
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- UPDATE
- UNSET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/ipsecparameter **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"ipsecparameter":{

"ikeversion":<String_value>,

"encalgo":<String[]_value>,

"hashalgo":<String[]_value>,

"lifetime":<Integer_value>,

"livenesscheckinterval":<Integer_value>,

"replaywindowsize":<Integer_value>,

"ikeretryinterval":<Integer_value>,

"perfectforwardsecrecy":<String_value>,

"retransmissiontime":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/ipsecparameter? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"ipsecparameter":{

"ikeversion":true,

"encalgo":true,

"hashalgo":true,

"lifetime":true,

"livenesscheckinterval":true,

"replaywindowsize":true,

"ikeretryinterval":true,

"perfectforwardsecrecy":true,

"retransmissiontime":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/ipsecparameter **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "ipsecparameter": [ {

"ikeversion":<String_value>,

"encalgo":<String[]_value>,

"hashalgo":<String[]_value>,

"lifetime":<Integer_value>,

"livenesscheckinterval":<Integer_value>,

"replaywindowsize":<Integer_value>,

"ikeretryinterval":<Integer_value>,

"perfectforwardsecrecy":<String_value>,

"responderonly":<String_value>,

"retransmissiontime":<Integer_value>,

"_nextgenapiresource":<String_value>
```

```
}]}
```

ipsecprofile

Configuration for IPSEC profile resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	The name of the ipsec profile. Minimum length = 1 Maximum length = 32
ikeversion	<String>	Read-write	IKE Protocol Version. Possible values = V1, V2
encalgo	<String[]>	Read-write	Type of encryption algorithm (Note: Selection of AES enables AES128). Possible values = AES, AES192, AES256
hashalgo	<String[]>	Read-write	Type of hashing algorithm. Possible values = HMAC_SHA1, HMAC_SHA256, HMAC_SHA384, HMAC_SHA512, HMAC_MD5

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
lifetime	<Integer>	Read-write	Lifetime of IKE SA in seconds. Lifetime of IPSec SA will be (lifetime of IKE SA/ 8). Minimum value = 480 Maximum value = 31536000
psk	<String>	Read-write	Pre shared key value.
publickey	<String>	Read-write	Public key file path.
privatekey	<String>	Read-write	Private key file path.
peerpublickey	<String>	Read-write	Peer public key file path.
livenesscheckinterval	<Integer>	Read-write	Number of seconds after which a notify payload is sent to check the liveliness of the peer. Additional retries are done as per retransmit interval setting. Zero value disables liveliness checks. Minimum value = 0 Maximum value = 64999
replaywindowsize	<Integer>	Read-write	IPSec Replay window size for the data traffic.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum value = 0 Maximum value = 16384
ikeretryinterval	<Integer>	Read-write	IKE retry interval for bringing up the connection. Minimum value = 60 Maximum value = 3600
retransmissiontime	<Integer>	Read-write	The interval in seconds to retry sending the IKE messages to peer, three consecutive attempts are done with doubled interval after every failure. Minimum value = 1 Maximum value = 99
perfectforwardsecrecy	<String>	Read-write	Enable/Disable PFS. Possible values = ENABLE, DISABLE
responderonly	<String>	Read-only	Responder Only config for IKED. Possible values = YES, NO
builtin	<String[]>	Read-only	Indicates that a variable is a built-in (SYSTEM INTERNAL) type.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL
feature	<String>	Read-only	The feature to be checked while applying this config.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- GET (ALL)
- GET
- COUNT
- DELETE

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/ipsecprofile **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"ipsecprofile":{

<b>"name":<String_value>,

</b>"ikeversion":<String_value>,

"encalgo":<String[]_value>,

"hashalgo":<String[]_value>,

"lifetime":<Integer_value>,

"psk":<String_value>,

"publickey":<String_value>,

"privatekey":<String_value>,

"peerpublickey":<String_value>,

"livenesscheckinterval":<Integer_value>,
```

```
"replaywindowsize":<Integer_value>,

"ikeretryinterval":<Integer_value>,

"retransmissiontime":<Integer_value>,

"perfectforwardsecrecy":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/ipsecprofile/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/ipsecprofile **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/ipsecprofile? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/ipsecprofile? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of ipsecprofile resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/ipsecprofile? **view=summary**

Use this query-parameter to get the summary output of ipsecprofile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/ipsecprofile? **pagesize=#no;pageno=#no**

Use this query-parameter to get the ipsecprofile resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "ipsecprofile": [ {

"name":<String_value>,

"ikeversion":<String_value>,

"encalgo":<String[]_value>,

"hashalgo":<String[]_value>,

"lifetime":<Integer_value>,

"livenesscheckinterval":<Integer_value>,

"replaywindowsize":<Integer_value>,
```

```
"retransmissiontime":<Integer_value>,

"psk":<String_value>,

"publickey":<String_value>,

"privatekey":<String_value>,

"peerpublickey":<String_value>,

"ikeretryinterval":<Integer_value>,

"perfectforwardsecrecy":<String_value>,

"responderonly":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/ipsecprofile/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/ipsecprofile/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/ipsecprofile/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of ipsecprofile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "ipsecprofile": [ {

"name":<String_value>,

"ikeversion":<String_value>,

"encalgo":<String[]_value>,

"hashalgo":<String[]_value>,

"lifetime":<Integer_value>,

"livenesscheckinterval":<Integer_value>,

"replaywindowsize":<Integer_value>,

"retransmissiontime":<Integer_value>,

"psk":<String_value>,

"publickey":<String_value>,

"privatekey":<String_value>,

"peerpublickey":<String_value>,

"ikeretryinterval":<Integer_value>,
```

```
"perfectforwardsecrecy":<String_value>,

"responderonly":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/ipsecprofile? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "ipsecprofile": [ { "__count": "#no"} ] }
```

ipsecalg

Ipsecalg

IPSECALG configuration.

NAME	DESCRIPTION
ipsecalgprofile	Configuration for IPSEC ALG profile
ipsecalgsession	Configuration for IPSEC ALG session

ipsecalgprofile

Configuration for IPSEC ALG profile resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	The name of the ipsec alg profile. Minimum length = 1 Maximum length = 32
ikesessiontimeout	<Integer>	Read-write	IKE session timeout in minutes. Default value: 60 Minimum value = 1 Maximum value = 1440
espsessiontimeout	<Integer>	Read-write	ESP session timeout in minutes. Default value: 60 Minimum value = 1 Maximum value = 1440

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
espgatetimeout	<Integer>	Read-write	Timeout ESP in seconds as no ESP packets are seen after IKE negotiation. Default value: 30 Minimum value = 3 Maximum value = 1200
connfailover	<String>	Read-write	Mode in which the connection failover feature must operate for the IPSec Alg. After a failover, established UDP connections and ESP packet flows are kept active and resumed on the secondary appliance. Recomended setting is ENABLED. Default value: ENABLED Possible values = ENABLED, DISABLED
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- UPDATE

- UNSET
- GET (ALL)
- GET
- COUNT
- DELETE

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/ipsecalgprofile **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"ipsecalgprofile":{

<b>"name":<String_value>,

</b>"ikesessiontimeout":<Integer_value>,

"espsessiontimeout":<Integer_value>,

"espgatetimeout":<Integer_value>,

"connfailover":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/ipsecalgprofile **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"ipsecalgprofile":{

<b>"name":<String_value>,

</b>"ikesessiontimeout":<Integer_value>,

"espsessiontimeout":<Integer_value>,

"espgatetimeout":<Integer_value>,
```

```
"connfailover":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/ipsecalgprofile? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"ipsecalgprofile":{

<b>"name":<String_value>,

</b>"ikesessiontimeout":true,

"espsessiontimeout":true,

"espgatetimeout":true,

"connfailover":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/ipsecalgprofile/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/ipsecalgprofile **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/ipsecalgprofile? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/ipsecalgprofile? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of ipsecalgprofile resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/ipsecalgprofile? **view=summary**

Use this query-parameter to get the summary output of ipsecalgprofile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/ipsecalgprofile? **pagesize=#no;pageno=#no**

Use this query-parameter to get the ipsecalgprofile resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "ipsecalgprofile": [ {

"name":<String_value>,

"ikesessiontimeout":<Integer_value>,

"espsessiontimeout":<Integer_value>,

"espgatetimeout":<Integer_value>,

"connfailover":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/ipsecalgprofile/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/ipsecalgprofile/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/ipsecalgprofile/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of ipsecalgprofile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "ipsecalgprofile": [ {

"name":<String_value>,

"ikesessiontimeout":<Integer_value>,

"espsessiontimeout":<Integer_value>,

"espgatetimeout":<Integer_value>,

"connfailover":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/ipsecalgprofile? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "ipsecalgprofile": [ { "__count": "#no"} ] }
```

ipsecalgsession

Configuration for IPSEC ALG session resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
sourceip_alg	<String>	Read-write	Original Source IP address. Minimum length = 1
natip_alg	<String>	Read-write	Natted Source IP address. Minimum length = 1
destip_alg	<String>	Read-write	Destination IP address. Minimum length = 1
sourceip	<String>	Read-write	Original Source IP address. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
natip	<String>	Read-write	Natted Source IP address. Minimum length = 1
destip	<String>	Read-write	Destination IP address. Minimum length = 1
spiin	<Integer>	Read-only	Client SPI for ESP.
spiout	<Integer>	Read-only	Server SPI for ESP.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET (ALL)
- COUNT
- FLUSH

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.
- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

FLUSH

URL: http:// <netscaler-ip-address> /nitro/v1/config/ipsecalgsession? **action=flush HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"ipsecalgsession":{

"sourceip":<String_value>,

"natip":<String_value>,

"destip":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/ipsecalgsession **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ipsecalgsession? **args=sourceip_alg: <String_value> ,natip_alg: <String_value> ,destip_alg: <String_value>**

Use this query-parameter to get ipsecalgsession resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/config/ipsecalgsession? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/ipsecalgsession? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of ipsecalgsession resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/ipsecalgsession? **view=summary**

Use this query-parameter to get the summary output of ipsecalgsession resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/ipsecalgsession? **pagesize=#no;pageno=#no**

Use this query-parameter to get the ipsecalgsession resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "ipsecalgsession": [ {

sourceip_alg:<String_value>,natip_alg:<String_value>,destip_alg:<String_va
lue>"sourceip":<String_value>,

"natip":<String_value>,

"destip":<String_value>,

"spiin":<Integer_value>,

"spiout":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/ipsecalgsession? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "ipsecalgsession": [ { "__count": "#no"} ] }
```

kafka

Kafka

Kafka Configuration

NAME	DESCRIPTION
kafkacluster	Configuration for Kafka cluster
kafkacluster_binding	Binding object showing the resources that can be bound to kafkacluster
kafkacluster_servicegroup_binding	Binding object showing the servicegroup that can be bound to kafkacluster

kafkacluster

Configuration for Kafka cluster resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the Kafka cluster. Minimum length = 1 Maximum length = 127
activesvc	<Integer>	Read-only	Total active services bound to servicegroup.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
totalsvc	<Integer>	Read-only	Total services bound to servicegroup.
topicname	<String>	Read-only	Topic of the servicegroup.
numtopics	<Integer>	Read-only	Total number of topic servicegroups bound.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/kafkacluster **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"kafkacluster":{

<b>"name":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/kafkacluster/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/kafkacluster **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/kafkacluster? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/kafkacluster? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of kafkacluster resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/kafkacluster? **view=summary**

Use this query-parameter to get the summary output of kafkacluster resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/kafkacluster? **pagesize=#no;pageno=#no**

Use this query-parameter to get the kafkacluster resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "kafkacluster": [ {

"name":<String_value>,

"activesvc":<Integer_value>,

"totalsvc":<Integer_value>,

"topicname":<String_value>,

"numtopics":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/kafkacluster/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/kafkacluster/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/kafkacluster/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of kafkacluster resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "kafkacluster": [ {

"name":<String_value>,

"activesvc":<Integer_value>,

"totalsvc":<Integer_value>,

"topicname":<String_value>,

"numtopics":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/kafkacluster? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "kafkacluster": [ { "__count": "#no"} ] }
```

kafkacluster_binding

Binding object which returns the resources bound to kafkacluster.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the Kafka cluster. Minimum length = 1 Maximum length = 127
kafkacluster_servicegroup_binding	<kafkacluster_servicegroup_binding[]>	Read-only	servicegroup that can be bound to kafkacluster.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/kafkacluster_binding/ name_value<String>
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "kafkacluster_binding": [ {

"name":<String_value>,

"kafkacluster_servicegroup_binding":<kafkacluster_servicegroup_binding[]_value>
```

```
}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/kafkacluster_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/kafkacluster_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "kafkacluster_binding": [ {

"name":<String_value>,

"kafkacluster_servicegroup_binding":<kafkacluster_servicegroup_binding[]_value>

}]}
```

kafkacluster_servicegroup_binding

Binding object showing the servicegroup that can be bound to kafkacluster.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
servicegroupname	<String>	Read-write	Name of the bound servicegroup.
name	<String>	Read-write	Name for the Kafka cluster. Minimum length = 1 Maximum length = 127
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT
- ADD
- DELETE

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of

creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/kafkacluster_servicegroup_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"kafkacluster_servicegroup_binding":{

<b>"name":<String_value>,

</b>"servicegroupname":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/kafkacluster_servicegroup_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ kafkacluster_servicegroup_binding/ name_value<String> ? **args=servicegroupname: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/kafkacluster_servicegroup_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ kafkacluster_servicegroup_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of kafkacluster_servicegroup_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/kafkacluster_servicegroup_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the kafkacluster_servicegroup_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "kafkacluster_servicegroup_binding": [ {

"servicegroupname":<String_value>,

"name":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/kafkacluster_servicegroup_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/kafkacluster_servicegroup_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "kafkacluster_servicegroup_binding": [ {

"servicegroupname":<String_value>,

"name":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/kafkacluster_servicegroup_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"kafkacluster_servicegroup_binding": [ { "__count": "#no"} ] }
```

lb

Load Balancing

Load Balancing configuration. The load balancing methods manage the selection of an appropriate physical server in a server farm.

NAME	DESCRIPTION
lbaction	Configuration for lb action
lbglobal_binding	Binding object showing the resources that can be bound to lbglobal
lbglobal_lbpolicy_binding	Binding object showing the lbpolicy that can be bound to lbglobal
lbgroup	Configuration for LB group
lbgroup_binding	Binding object showing the resources that can be bound to lbgroup
lbgroup_lbvserver_binding	Binding object showing the lbvserver that can be bound to lbgroup
lbmetrictable	Configuration for metric table
lbmetrictable_binding	Binding object showing the resources that can be bound to lbmetrictable
lbmetrictable_metric_binding	Binding object showing the metric that can be bound to lbmetrictable
lbmonbindings	Configuration for monitro bindings
lbmonbindings_binding	Binding object showing the resources that can be bound to lbmonbindings
lbmonbindings_gslbservicegroup_binding	Binding object showing the gslbservicegroup that can be bound to lbmonbindings

NAME	DESCRIPTION
lbmonbindings_service_binding	Binding object showing the service that can be bound to lbmonbindings
lbmonbindings_servicegroup_binding	Binding object showing the servicegroup that can be bound to lbmonbindings
lbmonitor	Configuration for monitor
lbmonitor_binding	Binding object showing the resources that can be bound to lbmonitor
lbmonitor_metric_binding	Binding object showing the metric that can be bound to lbmonitor
lbmonitor_service_binding	Binding object showing the service that can be bound to lbmonitor
lbmonitor_servicegroup_binding	Binding object showing the servicegroup that can be bound to lbmonitor
lbmonitor_sslcertkey_binding	Binding object showing the sslcertkey that can be bound to lbmonitor
lbparameter	Configuration for LB parameter
lbpersistentsessions	Configuration for persistence session
lbpolicy	Configuration for lb policy

NAME	DESCRIPTION
lbpolicy_binding	Binding object showing the resources that can be bound to lbpolicy
lbpolicy_gslbvserver_binding	Binding object showing the gslbvserver that can be bound to lbpolicy
lbpolicy_lbglobal_binding	Binding object showing the lbglobal that can be bound to lbpolicy
lbpolicy_lbpolicylabel_binding	Binding object showing the lbpolicylabel that can be bound to lbpolicy
lbpolicy_lbvserver_binding	Binding object showing the lbvserver that can be bound to lbpolicy
lbpolicylabel	Configuration for lb policy label
lbpolicylabel_binding	Binding object showing the resources that can be bound to lbpolicylabel
lbpolicylabel_lbpolicy_binding	Binding object showing the lbpolicy that can be bound to lbpolicylabel
lbpolicylabel_policybinding_binding	Binding object showing the policybinding that can be bound to lbpolicylabel
lbprofile	Configuration for LB profile
lbroute	Configuration for LB route
lbroute6	Configuration for LB route6

NAME	DESCRIPTION
lbsipparameters	Configuration for SIP parameters
lbvserver	Configuration for Load Balancing Virtual Server
lbvserver_analyticsprofile_binding	Binding object showing the analyticsprofile that can be bound to lbvserver
lbvserver_appflowpolicy_binding	Binding object showing the appflowpolicy that can be bound to lbvserver
lbvserver_appfwpolicy_binding	Binding object showing the appfwpolicy that can be bound to lbvserver
lbvserver_appqoepolicy_binding	Binding object showing the appqoepolicy that can be bound to lbvserver
lbvserver_auditnslogpolicy_binding	Binding object showing the auditnslogpolicy that can be bound to lbvserver
lbvserver_auditsyslogpolicy_binding	Binding object showing the auditsyslogpolicy that can be bound to lbvserver
lbvserver_authorizationpolicy_binding	Binding object showing the authorizationpolicy that can be bound to lbvserver
lbvserver_binding	Binding object showing the resources that can be bound to lbvserver

NAME	DESCRIPTION
lbvserver_botpolicy_binding	Binding object showing the botpolicy that can be bound to lbvserver
lbvserver_cachepolicy_binding	Binding object showing the cachepolicy that can be bound to lbvserver
lbvserver_cmppolicy_binding	Binding object showing the cmppolicy that can be bound to lbvserver
lbvserver_contentinspectionpolicy_binding	Binding object showing the contentinspectionpolicy that can be bound to lbvserver
lbvserver_csvserver_binding	Binding object showing the csvserver that can be bound to lbvserver
lbvserver_dnspolicy64_binding	Binding object showing the dnspolicy64 that can be bound to lbvserver
lbvserver_feopolicy_binding	Binding object showing the feopolicy that can be bound to lbvserver
lbvserver_lbpolicy_binding	Binding object showing the lbpolicy that can be bound to lbvserver
lbvserver_responderpolicy_binding	Binding object showing the responderpolicy that can be bound to lbvserver
lbvserver_rewritepolicy_binding	Binding object showing the rewritepolicy that can be bound to lbvserver

NAME	DESCRIPTION
lbvserver_service_binding	Binding object showing the service that can be bound to lbvserver
lbvserver_servicegroup_binding	Binding object showing the servicegroup that can be bound to lbvserver
lbvserver_servicegroupmember_binding	Binding object showing the servicegroupmember that can be bound to lbvserver
lbvserver_spilloverpolicy_binding	Binding object showing the spilloverpolicy that can be bound to lbvserver
lbvserver_tmtrafficpolicy_binding	Binding object showing the tmtrafficpolicy that can be bound to lbvserver
lbvserver_transformpolicy_binding	Binding object showing the transformpolicy that can be bound to lbvserver
lbvserver_videooptimizationdetectionpolicy_binding	Binding object showing the videooptimizationdetectionpolicy that can be bound to lbvserver
lbvserver_videooptimizationpacingpolicy_binding	Binding object showing the videooptimizationpacingpolicy that can be bound to lbvserver
lbwlm	Configuration for web log manager
lbwlm_binding	Binding object showing the resources that can be bound to lbwlm

NAME	DESCRIPTION
lbwlm_lbvserver_binding	Binding object showing the lbvserver that can be bound to lbwlm

lbaction

Configuration for lb action resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the LB action. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space ( ), at (@), equals (=), colon (:), and underscore characters. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my lb action" or 'my lb action').

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
type	<String>	Read-write	Type of an LB action. Available settings function as follows: * NOLBACTION - Does not consider LB action in making LB decision. * SELECTIONORDER - services bound to vserver with order specified in value parameter is considerd for lb/gslb decision. Possible values = NOLBACTION, SELECTIONORDER
value	<Integer[]>	Read-write	The selection order list used during lb/gslb decision. Preference of services during lb/gslb decision is as follows - services corresponding to first order specified in the sequence is considered first, services corresponding to second order specified in the sequence is considered next and

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			so on. For example, if -value 2 1 3 is specified here and service-1 bound to a vserver with order 1, service-2 bound to a vserver with order 2 and service-3 bound to a vserver with order 3. Then preference of selecting services in LB decision is as follows: service-2, service-1, service-3. Minimum value = 1
comment	<String>	Read-write	Comment. Any type of information about this LB action.
newname	<String>	Read-write	New name for the LB action. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space ( ), at (@), equals (=), colon (:), and underscore characters. The following requirement applies

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my lb action" or my lb action'). Minimum length = 1
hits	<Integer>	Read-only	The number of times the action has been taken.
referencecount	<Integer>	Read-only	The number of references to the action.
undefhits	<Integer>	Read-only	The number of times the action resulted in UNDEF.
feature	<String>	Read-only	The feature to be checked while applying this config.
builtin	<String[]>	Read-only	Flag to determine whether LB action is built-in or not. Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL
_nextgenapiresource	<String>	Read-only	.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT
- RENAME

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbaction **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"lbaction":{

<b>"name":<String_value>,

</b><b>"type":<String_value>,

</b>"value":<Integer[]_value>,

"comment":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbaction/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbaction **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"lbaction":{

<b>"name":<String_value>,

</b>"value":<Integer[]_value>,

"comment":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbaction? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"lbaction":{

<b>"name":<String_value>,

</b>"comment":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

RENAME

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbaction? **action=rename HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"lbaction":{

<b>"name":<String_value>,

</b><b>"newname":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbaction **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/lbaction? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/lbaction? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of lbaction resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/lbaction? **view=summary**

Use this query-parameter to get the summary output of lbaction resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/lbaction? **pagesize=#no;pageno=#no**

Use this query-parameter to get the lbaction resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "lbaction": [ {

"name":<String_value>,
```

```
"type":<String_value>,

"value":<Integer[]_value>,

"hits":<Integer_value>,

"referencecount":<Integer_value>,

"undefhits":<Integer_value>,

"comment":<String_value>,

"feature":<String_value>,

"builtin":<String[]_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbaction/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/lbaction/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/lbaction/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of lbaction resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lbaction": [ {

"name":<String_value>,

"type":<String_value>,

"value":<Integer[]_value>,

"hits":<Integer_value>,

"referencecount":<Integer_value>,

"undefhits":<Integer_value>,

"comment":<String_value>,

"feature":<String_value>,

"builtin":<String[]_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbaction? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "lbaction": [ { "__count": "#no"} ] }
```

lbglobal_binding

Binding object which returns the resources bound to lbglobal.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
lbglobal_lbpolicy_binding	<lbglobal_lbpolicy_binding[]>	Read-write	lbpolicy that can be bound to lbglobal.

Operations

(click to see Properties)

- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbglobal_binding

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "lbglobal_binding": [ {

"lbglobal_lbpolicy_binding":<lbglobal_lbpolicy_binding[]_value>
```

```
}]}
```

lbglobal_lbpolicy_binding

Binding object showing the lbpolicy that can be bound to lbglobal.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
priority	<Integer>	Read-write	Specifies the priority of the policy.
labeltype	<String>	Read-write	Type of invocation, Available settings function as follows: * vserver - Invokes the unnamed policy label associated with the specified virtual server. * policylabel - Invoke the specified policy label. Possible values = reqvserver, policylabel
labelname	<String>	Read-write	Name of the virtual server or user-defined policy label to invoke if the policy evaluates to TRUE.
type	<String>	Read-write	. Possible values = REQ_OVERRIDE, REQ_DEFAULT,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			OTHERTCP_REQ_OVERRIDE, OTHERTCP_REQ_DEFAULT, SIPUDP_REQ_OVERRIDE, SIPUDP_REQ_DEFAULT, SIPTCP_REQ_OVERRIDE, SIPTCP_REQ_DEFAULT, MSSQL_REQ_OVERRIDE, MSSQL_REQ_DEFAULT, MYSQL_REQ_OVERRIDE, MYSQL_REQ_DEFAULT, ORACLE_REQ_OVERRIDE, ORACLE_REQ_DEFAULT, NAT_REQ_OVERRIDE, NAT_REQ_DEFAULT, DIAMETER_REQ_OVERRIDE, DIAMETER_REQ_DEFAULT, RADIUS_REQ_OVERRIDE, RADIUS_REQ_DEFAULT,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			DNS_REQ_OVERRIDE, DNS_REQ_DEFAULT, MQTT_REQ_OVERRIDE, MQTT_REQ_DEFAULT, QUIC_OVERRIDE, QUIC_DEFAULT, HTTPQUIC_REQ_OVERRIDE, HTTPQUIC_REQ_DEFAULT, GSLB_REQ_OVERRIDE, GSLB_REQ_DEFAULT
invoke	<Boolean>	Read-write	If the current policy evaluates to TRUE, terminate evaluation of policies bound to the current policy label, and then forward the request to the specified virtual server or evaluate the specified policy label.
gotopriorityexpression	<String>	Read-write	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
policyname	<String>	Read-write	Name of the LB policy.
globalbindtype	<String>	Read-write	. Default value: SYSTEM_GLOBAL Possible values = SYSTEM_GLOBAL, VPN_GLOBAL, RNAT_GLOBAL, APPFW_GLOBAL, TM_GLOBAL
flowtype	<Integer>	Read-only	flowtype of the bound LB policy.
numpol	<Integer>	Read-only	number of polices bound to label.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/lbglobal_lbpolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"lbglobal_lbpolicy_binding":{

<b>"policyname":<String_value>,

</b><b>"priority":<Integer_value>,

</b>"type":<String_value>,

"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>,
```

```
"labeltype":<String_value>,

"labelname":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbglobal_lbpolicy_binding **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/lbglobal_lbpolicy_binding? **args= policyname:<String_value>, type: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbglobal_lbpolicy_binding **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/lbglobal_lbpolicy_binding? **args=type: <String_value>**

Use this query-parameter to get lbglobal_lbpolicy_binding resources based on additional properties.

filter http:// <netscaler-ip-address> /nitro/v1/config/lbglobal_lbpolicy_binding? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of lbglobal_lbpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/lbglobal_lbpolicy_binding? **pagesize=#no;pageno=#no**

Use this query-parameter to get the lbglobal_lbpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lbglobal_lbpolicy_binding": [ {

"priority":<Integer_value>,

"labeltype":<String_value>,

"labelname":<String_value>,

"type":<String_value>,

"invoke":<Boolean_value>,

"gotopriorityexpression":<String_value>,

"policyname":<String_value>,

"globalbindtype":<String_value>,

"flowtype":<Integer_value>,
```

```
"numpol":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbglobal_lbpolicy_binding? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "lbglobal_lbpolicy_binding": [ { "__count": "#no"} ] }
```

lbgroup

Configuration for LB group resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the load balancing virtual server group. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
persistencetype	<String>	Read-write	Type of persistence for the group. Available settings function as follows: * SOURCEIP - Create persistence sessions based on the client IP. * COOKIEINSERT - Create persistence sessions based on a cookie in client requests. The cookie is inserted by a Set-Cookie directive from the server, in its first response to a client. * RULE - Create persistence sessions based on a user defined rule. * NONE - Disable persistence for the group. Possible values = SOURCEIP, COOKIEINSERT, RULE, NONE
persistencebackup	<String>	Read-write	Type of backup persistence for the group.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = SOURCEIP, NONE
backuppersistencetimeout	<Integer>	Read-write	Time period, in minutes, for which backup persistence is in effect. Default value: 2 Minimum value = 2 Maximum value = 1440
persistmask	<String>	Read-write	Persistence mask to apply to source IPv4 addresses when creating source IP based persistence sessions. Minimum length = 1
cookiename	<String>	Read-write	Use this parameter to specify the cookie name for COOKIE peristence type. It specifies the name of cookie with a maximum of 32 characters. If not specified, cookie name is internally generated.
v6persistmasklen	<Integer>	Read-write	Persistence mask to apply to source IPv6 addresses when creating source IP based persistence sessions.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: 128 Minimum value = 1 Maximum value = 128
cookiedomain	<String>	Read-write	Domain attribute for the HTTP cookie. Minimum length = 1
timeout	<Integer>	Read-write	Time period for which a persistence session is in effect. Default value: 2 Minimum value = 0 Maximum value = 1440
rule	<String>	Read-write	Expression, or name of a named expression, against which traffic is evaluated. The following requirements apply only to the Citrix ADC CLI: * If the expression includes one or more spaces, enclose the entire expression in double quotation marks.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			* If the expression itself includes double quotation marks, escape the quotations by using the \ character. * Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks. Default value: "None"
mastervserver	<String>	Read-write	When USE_VSERVER_PERSISTENCE is enabled, one can use this setting to designate a member vserver as master which is responsible to create the persistence sessions.
usevserverpersistency	<String>	Read-write	Use this parameter to enable vserver level persistence on group members. This allows member vservers to have their own persistence, but need to be

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			compatible with other members persistence rules. When this setting is enabled persistence sessions created by any of the members can be shared by other member vservers. Default value: DISABLED Possible values = ENABLED, DISABLED
newname	<String>	Read-write	New name for the load balancing virtual server group. Minimum length = 1
td	<Integer>	Read-only	Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0. Minimum value = 0 Maximum value = 4094
_nextgenapiresource	<String>	Read-only	.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- UPDATE
- UNSET
- DELETE
- GET (ALL)
- GET
- COUNT
- RENAME

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbgroup **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"lbgroup":{

<b>"name":<String_value>,

</b>"persistencetype":<String_value>,

"persistencebackup":<String_value>,

"backuppersistencetimeout":<Integer_value>,

"persistmask":<String_value>,

"cookiename":<String_value>,

"v6persistmasklen":<Integer_value>,

"cookiedomain":<String_value>,

"timeout":<Integer_value>,

"rule":<String_value>,

"mastervserver":<String_value>,

"usevserverpersistency":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbgroup **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"lbgroup":{

<b>"name":<String_value>,

</b>"persistencetype":<String_value>,

"persistencebackup":<String_value>,

"backuppersistencetimeout":<Integer_value>,

"persistmask":<String_value>,

"cookiename":<String_value>,

"v6persistmasklen":<Integer_value>,

"cookiedomain":<String_value>,

"timeout":<Integer_value>,

"rule":<String_value>,

"usevserverpersistency":<String_value>,

"mastervserver":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbgroup? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"lbgroup":{

<b>"name":<String_value>,

</b>"persistencetype":true,

"persistencebackup":true,

"backuppersistencetimeout":true,

"persistmask":true,

"cookiename":true,

"v6persistmasklen":true,

"cookiedomain":true,

"timeout":true,

"rule":true,

"usevserverpersistency":true,

"mastervserver":true
```

```
}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbgroup/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

RENAME

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbgroup? **action=rename HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"lbgroup":{

<b>"name":<String_value>,

</b><b>"newname":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbgroup **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/lbgroup? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/lbgroup? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of lbgroup resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/lbgroup? **view=summary**

Use this query-parameter to get the summary output of lbgroup resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/lbgroup? **pagesize=#no;pageno=#no**

Use this query-parameter to get the lbgroup resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "lbgroup": [ {

"name":<String_value>,

"persistencetype":<String_value>,

"persistencebackup":<String_value>,

"backuppersistencetimeout":<Integer_value>,

"persistmask":<String_value>,

"v6persistmasklen":<Integer_value>,

"cookiename":<String_value>,

"cookiedomain":<String_value>,

"timeout":<Integer_value>,

"rule":<String_value>,

"td":<Integer_value>,

"usevserverpersistency":<String_value>,

"mastervserver":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbgroup/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/lbgroup/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/lbgroup/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of lbgroup resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lbgroup": [ {

"name":<String_value>,

"persistencetype":<String_value>,

"persistencebackup":<String_value>,

"backuppersistencetimeout":<Integer_value>,

"persistmask":<String_value>,

"v6persistmasklen":<Integer_value>,

"cookiename":<String_value>,

"cookiedomain":<String_value>,

"timeout":<Integer_value>,

"rule":<String_value>,
```

```
"td":<Integer_value>,

"usevserverpersistency":<String_value>,

"mastervserver":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbgroup? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "lbgroup": [ { "__count": "#no"} ] }
```

lbgroup_binding

Binding object which returns the resources bound to lbgroup.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the load balancing virtual server group. Minimum length = 1
lbgroup_lbvserver_binding	<lbgroup_lbvserver_binding[]>	Read-only	lbvserver that can be bound to lbgroup.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbgroup_binding/ name_value<String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "lbgroup_binding": [ {

"name":<String_value>,

"lbgroup_lbvserver_binding":<lbgroup_lbvserver_binding[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbgroup_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/lbgroup_binding?**bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "lbgroup_binding": [ {

"name":<String_value>,

"lbgroup_lbvserver_binding":<lbgroup_lbvserver_binding[]_value>

}]}
```

lbgroup_lbvserver_binding

Binding object showing the lbvserver that can be bound to lbgroup.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
vservername	<String>	Read-write	Virtual server name.
name	<String>	Read-write	Name for the load balancing virtual server group. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Can be changed after the virtual server is created.

CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my lbgroup" or 'my lbgroup').

Minimum length = 1

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of

creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/lbgroup_lbvserver_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"lbgroup_lbvserver_binding":{

<b>"name":<String_value>,

</b><b>"vservername":<String_value></b>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbgroup_lbvserver_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ lbgroup_lbvserver_binding/ name_value<String> ? **args= vservername:<String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbgroup_lbvserver_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ lbgroup_lbvserver_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of lbgroup_lbvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/lbgroup_lbvserver_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the lbgroup_lbvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lbgroup_lbvserver_binding": [ {

"vservername":<String_value>,

"name":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbgroup_lbvserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/lbgroup_lbvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lbgroup_lbvserver_binding": [ {

"vservername":<String_value>,
```

```
"name":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbgroup_lbvserver_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"lbgroup_lbvserver_binding": [ { "__count": "#no"} ] }
```

lbmetrictable

Configuration for metric table resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
metrictable	<String>	Read-write	Name for the metric table. Must begin with an ASCII alphanumeric or

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my metrictable" or 'my metrictable'). Minimum length = 1 Maximum length = 31
metric	<String>	Read-write	Name of the metric for which to change the SNMP OID. Minimum length = 1
Snmpoid	<String>	Read-write	New SNMP OID of the metric. Minimum length = 1
metrictype	<String>	Read-only	Indication if it is a configured or internal.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = INTERNAL, CONFIGURED
builtin	<String[]>	Read-only	. Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL
feature	<String>	Read-only	The feature to be checked while applying this config.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbmetrictable **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"lbmetrictable":{

<b>"metrictable":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbmetrictable/ metrictable_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbmetrictable **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"lbmetrictable":{

<b>"metrictable":<String_value>,

</b><b>"metric":<String_value>,

</b><b>"Snmpoid":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbmetrictable **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/lbmetrictable? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/lbmetrictable? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of lbmetrictable resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/lbmetrictable? **view=summary**

Use this query-parameter to get the summary output of lbmetrictable resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/lbmetrictable? **pagesize=#no;pageno=#no**

Use this query-parameter to get the lbmetrictable resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "lbmetrictable": [ {

"metrictable":<String_value>,

"metric":<String_value>,
```

```
"Snmpoid":<String_value>,

"flags":<Boolean_value>,

"metrictype":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbmetrictable/ metrictable_value<String>
Query-parameters: attrs http:// <netscaler-ip-address> /nitro/v1/config/lbmetrictable/ metrictable_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/lbmetrictable/ metrictable_value<String> ? **view=summary**

Use this query-parameter to get the summary output of lbmetrictable resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lbmetrictable": [ {

"metrictable":<String_value>,

"metric":<String_value>,

"Snmpoid":<String_value>,

"flags":<Boolean_value>,

"metrictype":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbmetrictable? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "lbmetrictable": [ { "__count": "#no"} ] }
```

lbmetrictable_binding

Binding object which returns the resources bound to lbmetrictable.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
metrictable	<String>	Read-write	Name of the metric table. Minimum length = 1 Maximum length = 31
lbmetrictable_metric_binding	<lbmetrictable_metric_binding[]>	Read-only	metric that can be bound to lbmetrictable.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbmetrictable_binding/ metrictable_value<String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "lbmetrictable_binding": [ {

"metrictable":<String_value>,

"lbmetrictable_metric_binding":<lbmetrictable_metric_binding[]_value>
```

```
}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbmetrictable_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/lbmetrictable_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "lbmetrictable_binding": [ {

"metrictable":<String_value>,

"lbmetrictable_metric_binding":<lbmetrictable_metric_binding[]_value>

}]}
```

lbmetrictable_metric_binding

Binding object showing the metric that can be bound to lbmetrictable.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
Snmpoid	<String>	Read-write	New SNMP OID of the metric. Minimum length = 1
metric	<String>	Read-write	Name of the metric for which to change the SNMP OID. Minimum length = 1
metrictable	<String>	Read-write	Name of the metric table. Minimum length = 1 Maximum length = 31
metrictype	<String>	Read-only	Indication if it is a configured or internal. Possible values = INTERNAL, CONFIGURED
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/lbmetrictable_metric_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"lbmetrictable_metric_binding":{

<b>"metrictable":<String_value>,
```

```
</b><b>"metric":<String_value>,

</b><b>"Snmpoid":<String_value></b>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbmetrictable_metric_binding/ metrictable_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ lbmetrictable_metric_binding/ metrictable_value<String> ? **args= metric:<String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbmetrictable_metric_binding/ metrictable_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ lbmetrictable_metric_binding/ metrictable_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of lbmetrictable_metric_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/lbmetrictable_metric_binding/ metrictable_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the lbmetrictable_metric_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lbmetrictable_metric_binding": [ {

"Snmpoid":<String_value>,

"metric":<String_value>,

"metrictable":<String_value>,

"metrictype":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbmetrictable_metric_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/lbmetrictable_metric_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lbmetrictable_metric_binding": [ {

"Snmpoid":<String_value>,

"metric":<String_value>,

"metrictable":<String_value>,

"metrictype":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbmetrictable_metric_binding/ metrictable_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"lbmetrictable_metric_binding": [ { "__count": "#no"} ] }
```

lbmonbindings

Configuration for monitro bindings resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
monitorname	<String>	Read-write	The name of the monitor. Minimum length = 1
type	<String>	Read-only	The type of monitor. Possible values = PING, TCP, HTTP, TCP-ECV, HTTP-ECV, UDP-ECV, DNS, FTP, LDNS-PING, LDNS-TCP, LDNS-DNS, RADIUS, USER, HTTP-INLINE, SIP-UDP, SIP-TCP, LOAD, FTP-EXTENDED, SMTP, SNMP, NNTP, MYSQL, MYSQL-ECV, MSSQL-ECV, ORACLE-ECV, LDAP, POP3, CITRIX-XML-SERVICE, CITRIX-

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			WEB-INTERFACE, DNS-TCP, RTSP, ARP, CITRIX-AG, CITRIX-AAC-LOGINPAGE, CITRIX-AAC-LAS, CITRIX-XD-DDC, ND6, CITRIX-WI-EXTENDED, DIAMETER, RADIUS_ACCOUNTING, STOREFRONT, APPC, SMPP, CITRIX-XNC-ECV, CITRIX-XDM, CITRIX-STA-SERVICE, CITRIX-STA-SERVICE-NHOP, MQTT, HTTP2, DTLS, QUIC, KAFKA-AUTODISCOVER
state	<String>	Read-only	The state of the monitor. Possible values = ENABLED, DISABLED
boundservicegroups vrstate	<String>	Read-only	The state of the servicegroup. Possible values = ENABLED, DISABLED
_nextgenapiresource	<String>	Read-only	.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbmonbindings **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/lbmonbindings? **args= monitorname:<String_value>,**

Use this query-parameter to get lbmonbindings resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/config/lbmonbindings? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/lbmonbindings? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of lbmonbindings resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/lbmonbindings? **view=summary**

Use this query-parameter to get the summary output of lbmonbindings resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/lbmonbindings? **pagesize=#no;pageno=#no**

Use this query-parameter to get the lbmonbindings resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "lbmonbindings": [ {

<b>monitorname:<String_value>,</b>"type":<String_value>,

"state":<String_value>,

"boundservicegroupsvrstate":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbmonbindings/ monitorname_value<String>
Query-parameters: attrs http:// <netscaler-ip-address> /nitro/v1/config/lbmonbindings/ monitorname_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/lbmonbindings/ monitorname_value<String> ? **view=summary**

Use this query-parameter to get the summary output of lbmonbindings resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lbmonbindings": [ {

<b>monitorname:<String_value>,</b>"type":<String_value>,

"state":<String_value>,

"boundservicegroupsvrstate":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbmonbindings? **args= monitorname:<String_value>, ;count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "lbmonbindings": [ { "__count": "#no"} ] }
```

lbmonbindings_binding

Binding object which returns the resources bound to lbmonbindings.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
monitorname	<String>	Read-write	The name of the monitor. Minimum length = 1
lbmonbindings_servicegroup_binding	<lbmonbindings_servicegroup_binding[]>	Read-only	servicegroup that can be bound to lbmonbindings.
lbmonbindings_gslbservicegroup_binding	<lbmonbindings_gslbservicegroup_binding[]>	Read-only	gslbservicegroup that can be bound to lbmonbindings.
lbmonbindings_service_binding	<lbmonbindings_service_binding[]>	Read-only	service that can be bound to lbmonbindings.

Operations

(click to see Properties)

- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of

creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbmonbindings_binding/ monitorname_value<String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "lbmonbindings_binding": [ {

"monitorname":<String_value>,

"lbmonbindings_servicegroup_binding":<lbmonbindings_servicegroup_binding[]
_value>,

"lbmonbindings_gslbservicegroup_binding":<lbmonbindings_gslbservicegroup_b
```

```
inding[]_value>,

"lbmonbindings_service_binding":<lbmonbindings_service_binding[]_value>

}]}
```

lbmonbindings_gslbservicegroup_binding

Binding object showing the gslbservicegroup that can be bound to lbmonbindings.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
monitorname	<String>	Read-write	The name of the monitor. Minimum length = 1
servicegroupname	<String>	Read-write	The name of the service group.
boundservicegroups vrstate	<String>	Read-only	The state of the servicegroup. Possible values = ENABLED, DISABLED
monstate	<String>	Read-only	The configured state (enable/disable) of Monitor on this service. Possible values = ENABLED, DISABLED
servicetype	<String>	Read-only	The type of service. Possible values = HTTP, FTP, TCP, UDP, SSL, SSL_BRIDGE,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			SSL_TCP, DTLS, NNTP, RPCSVR, DNS, ADNS, SNMP, RTSP, DHCPRA, ANY, SIP_UDP, SIP_TCP, SIP_SSL, DNS_TCP, ADNS_TCP, MYSQL, MSSQL, ORACLE, MONGO, MONGO_TLS, RADIUS, RADIUSListener, RDP, DIAMETER, SSL_DIAMETER, TFTP, SMPP, PPTP, GRE, SYSLOGTCP, SYSLOGUDP, FIX, SSL_FIX, USER_TCP, USER_SSL_TCP, QUIC, IPFIX, LOGSTREAM, LOGSTREAM_SSL, MQTT, MQTT_TLS, QUIC_BRIDGE, DOT, ADNS_DOT, HTTP_QUIC, ADNS_DOH, KAFKA_BROKER
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbmonbindings_gslbservicegroup_binding/ monitorname_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/ config/lbmonbindings_gslbservicegroup_binding/ monitorname_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of lbmonbindings_gslbservicegroup_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ lbmonbindings_gslbservicegroup_binding/ monitorname_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the lbmonbindings_gslbservicegroup_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lbmonbindings_gslbservicegroup_binding": [ {

"monitorname":<String_value>,

"servicegroupname":<String_value>,

"boundservicegroupsvrstate":<String_value>,

"monstate":<String_value>,

"servicetype":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbmonbindings_gslbservicegroup_binding/ monitorname_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"lbmonbindings_gslbservicegroup_binding": [ { "__count": "#no"} ] }
```

lbmonbindings_service_binding

Binding object showing the service that can be bound to lbmonbindings.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
servicename	<String>	Read-write	The name of the service.
monitorname	<String>	Read-write	The name of the monitor. Minimum length = 1
servicetype	<String>	Read-only	The type of service. Possible values = HTTP, FTP, TCP, UDP, SSL, SSL_BRIDGE, SSL_TCP, DTLS, NNTP, RPCSVR,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			DNS, ADNS, SNMP, RTSP, DHCPRA, ANY, SIP_UDP, SIP_TCP, SIP_SSL, DNS_TCP, ADNS_TCP, MYSQL, MSSQL, ORACLE, MONGO, MONGO_TLS, RADIUS, RADIUSListener, RDP, DIAMETER, SSL_DIAMETER, TFTP, SMPP, PPTP, GRE, SYSLOGTCP, SYSLOGUDP, FIX, SSL_FIX, USER_TCP, USER_SSL_TCP, QUIC, IPFIX, LOGSTREAM, LOGSTREAM_SSL, MQTT, MQTT_TLS, QUIC_BRIDGE, DOT, ADNS_DOT, HTTP_QUIC, ADNS_DOH, KAFKA_BROKER
port	<Integer>	Read-only	The port of the service. Range 1 - 65535 * in CLI is represented as

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			65535 in NITRO API
ipaddress	<String>	Read-only	The IPAddress of the service.
svrstate	<String>	Read-only	The state of the service. Possible values = UP, DOWN, UNKNOWN, BUSY, OUT OF SERVICE, GOING OUT OF SERVICE, DOWN WHEN GOING OUT OF SERVICE, NS_EMPTY_STR, Unknown, DISABLED
monsvcstate	<String>	Read-only	The configured state (enable/disable) of Monitor on this service. Possible values = ENABLED, DISABLED
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbmonbindings_service_binding/ monitorname_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/ config/lbmonbindings_service_binding/ monitorname_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of lbmonbindings_service_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/lbmonbindings_service_binding/ monitorname_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the lbmonbindings_service_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lbmonbindings_service_binding": [ {

"servicename":<String_value>,

"monitorname":<String_value>,

"servicetype":<String_value>,

"port":<Integer_value>,

"ipaddress":<String_value>,

"svrstate":<String_value>,

"monsvcstate":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbmonbindings_service_binding/ monitorname_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"lbmonbindings_service_binding": [ { "__count": "#no"} ] }
```

lbmonbindings_servicegroup_binding

Binding object showing the servicegroup that can be bound to lbmonbindings.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
monitorname	<String>	Read-write	The name of the monitor. Minimum length = 1
servicegroupname	<String>	Read-write	The name of the service group.
boundservicegroups vrstate	<String>	Read-only	The state of the servicegroup. Possible values = ENABLED, DISABLED
servicetype	<String>	Read-only	The type of service. Possible values = HTTP, FTP, TCP, UDP, SSL, SSL_BRIDGE, SSL_TCP, DTLS,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			NNTP, RPCSVR, DNS, ADNS, SNMP, RTSP, DHCPRA, ANY, SIP_UDP, SIP_TCP, SIP_SSL, DNS_TCP, ADNS_TCP, MYSQL, MSSQL, ORACLE, MONGO, MONGO_TLS, RADIUS, RADIUSListener, RDP, DIAMETER, SSL_DIAMETER, TFTP, SMPP, PPTP, GRE, SYSLOGTCP, SYSLOGUDP, FIX, SSL_FIX, USER_TCP, USER_SSL_TCP, QUIC, IPFIX, LOGSTREAM, LOGSTREAM_SSL, MQTT, MQTT_TLS, QUIC_BRIDGE, DOT, ADNS_DOT, HTTP_QUIC, ADNS_DOH, KAFKA_BROKER
monstate	<String>	Read-only	The configured state (enable/disable) of Monitor on this service.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ENABLED, DISABLED
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbmonbindings_servicegroup_binding/ monitorname_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/ config/lbmonbindings_servicegroup_binding/ monitorname_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of lbmonbindings_servicegroup_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/lbmonbindings_servicegroup_binding/ monitorname_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the lbmonbindings_servicegroup_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lbmonbindings_servicegroup_binding": [ {

"monitorname":<String_value>,

"servicegroupname":<String_value>,

"boundservicegroupsvrstate":<String_value>,

"servicetype":<String_value>,

"monstate":<String_value>
```

```
}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbmonbindings_servicegroup_binding/monitorname_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"lbmonbindings_servicegroup_binding": [ { "__count": "#no"} ] }
```

lbmonitor

Configuration for monitor resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
monitorname	<String>	Read-write	Name for the monitor. Must begin with an ASCII alphanumeric or underscore (_) character, and must

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my monitor" or 'my monitor'). Minimum length = 1
type	<String>	Read-write	Type of monitor that you want to create. Possible values = PING, TCP, HTTP, TCP-ECV, HTTP-ECV, UDP-ECV, DNS, FTP, LDNS-PING, LDNS-TCP, LDNS-DNS, RADIUS, USER, HTTP-INLINE, SIP-UDP, SIP-TCP, LOAD, FTP-EXTENDED, SMTP, SNMP, NNTP, MYSQL, MYSQL-ECV, MSSQL-ECV, ORACLE-ECV,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			LDAP, POP3, CITRIX-XML-SERVICE, CITRIX-WEB-INTERFACE, DNS-TCP, RTSP, ARP, CITRIX-AG, CITRIX-AAC-LOGINPAGE, CITRIX-AAC-LAS, CITRIX-XD-DDC, ND6, CITRIX-WI-EXTENDED, DIAMETER, RADIUS_ACCOUNTING, STOREFRONT, APPC, SMPP, CITRIX-XNC-ECV, CITRIX-XDM, CITRIX-STA-SERVICE, CITRIX-STA-SERVICE-NHOP, MQTT, HTTP2, DTLS, QUIC, KAFKA-AUTODISCOVER
action	<String>	Read-write	Action to perform when the response to an inline monitor (a monitor of type HTTP-INLINE) indicates that the service is down. A service monitored by an inline monitor is considered DOWN if

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			the response code is not one of the codes that have been specified for the Response Code parameter. Available settings function as follows: * NONE - Do not take any action. However, the show service command and the show lb monitor command indicate the total number of responses that were checked and the number of consecutive error responses received after the last successful probe. * LOG - Log the event in NSLOG or SYSLOG. * DOWN - Mark the service as being down, and then do not direct any traffic to the service until the configured down time has expired. Persistent connections to the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			service are terminated as soon as the service is marked as DOWN. Also, log the event in NSLOG or SYSLOG. Default value: DOWN Possible values = NONE, LOG, DOWN
respcode	<String[]>	Read-write	Response codes for which to mark the service as UP. For any other response code, the action performed depends on the monitor type. HTTP monitors and RADIUS monitors mark the service as DOWN, while HTTP-INLINE monitors perform the action indicated by the Action parameter.
httprequest	<String>	Read-write	HTTP request to send to the server (for example, "HEAD /file.html").
rtsprequest	<String>	Read-write	RTSP request to send to the server (for example, "OPTIONS *").

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
customheaders	<String>	Read-write	Custom header string to include in the monitoring probes.
maxforwards	<Integer>	Read-write	Maximum number of hops that the SIP request used for monitoring can traverse to reach the server. Applicable only to monitors of type SIP-UDP. Default value: 1 Minimum value = 0 Maximum value = 255
sipmethod	<String>	Read-write	SIP method to use for the query. Applicable only to monitors of type SIP-UDP. Possible values = OPTIONS, INVITE, REGISTER
sipuri	<String>	Read-write	SIP URI string to send to the service (for example, sip:sip.test). Applicable only to monitors of type SIP-UDP. Minimum length = 1
sipreguri	<String>	Read-write	SIP user to be registered. Applicable only if the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			monitor is of type SIP-UDP and the SIP Method parameter is set to REGISTER. Minimum length = 1
send	<String>	Read-write	String to send to the service. Applicable to TCP-ECV, HTTP-ECV, and UDP-ECV monitors.
recv	<String>	Read-write	String expected from the server for the service to be marked as UP. Applicable to TCP-ECV, HTTP-ECV, and UDP-ECV monitors.
query	<String>	Read-write	Domain name to resolve as part of monitoring the DNS service (for example, example.com).
querytype	<String>	Read-write	Type of DNS record for which to send monitoring queries. Set to Address for querying A records, AAAA for querying AAAA records, and Zone for querying the SOA record. Possible values = Address, Zone, AAAA

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
scriptname	<String>	Read-write	Path and name of the script to execute. The script must be available on the Citrix ADC, in the /nsconfig/monitors/ directory. Minimum length = 1
scriptargs	<String>	Read-write	String of arguments for the script. The string is copied verbatim into the request.
secureargs	<String>	Read-write	List of arguments for the script which should be secure.
dispatcherip	<String>	Read-write	IP address of the dispatcher to which to send the probe.
dispatcherport	<Integer>	Read-write	Port number on which the dispatcher listens for the monitoring probe.
username	<String>	Read-write	User name with which to probe the RADIUS, NNTP, FTP, FTP-EXTENDED, MYSQL, MSSQL, POP3, CITRIX-AG, CITRIX-XD-DDC, CITRIX-WI-EXTENDED, CITRIX-XNC or CITRIX-XDM server.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum length = 1
password	<String>	Read-write	Password that is required for logging on to the RADIUS, NNTP, FTP, FTP-EXTENDED, MYSQL, MSSQL, POP3, CITRIX-AG, CITRIX-XD-DDC, CITRIX-WI-EXTENDED, CITRIX-XNC-ECV or CITRIX-XDM server. Used in conjunction with the user name specified for the User Name parameter. Minimum length = 1
secondarypassword	<String>	Read-write	Secondary password that users might have to provide to log on to the Access Gateway server. Applicable to CITRIX-AG monitors.
logonpointname	<String>	Read-write	Name of the logon point that is configured for the Citrix Access Gateway Advanced Access Control software. Required if you want to monitor the associated login page or Logon Agent. Applicable to CITRIX-AAC-LAS and CITRIX-AAC-

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			LOGINPAGE monitors.
lasversion	<String>	Read-write	Version number of the Citrix Advanced Access Control Logon Agent. Required by the CITRIX-AAC-LAS monitor.
radkey	<String>	Read-write	Authentication key (shared secret text string) for RADIUS clients and servers to exchange. Applicable to monitors of type RADIUS and RADIUS_ACCOUNTING. Minimum length = 1
radnasid	<String>	Read-write	NAS-Identifier to send in the Access-Request packet. Applicable to monitors of type RADIUS. Minimum length = 1
radnasip	<String>	Read-write	Network Access Server (NAS) IP address to use as the source IP address when monitoring a RADIUS server. Applicable to monitors of type RADIUS and

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			RADIUS_ACCOUNTING.
radaccounttype	<Integer>	Read-write	Account Type to be used in Account Request Packet. Applicable to monitors of type RADIUS_ACCOUNTING. Default value: 1 Minimum value = 0 Maximum value = 15
radframedip	<String>	Read-write	Source ip with which the packet will go out . Applicable to monitors of type RADIUS_ACCOUNTING.
radapn	<String>	Read-write	Called Station Id to be used in Account Request Packet. Applicable to monitors of type RADIUS_ACCOUNTING. Minimum length = 1
radmsisdn	<String>	Read-write	Calling Stations Id to be used in Account Request Packet. Applicable to monitors of type RADIUS_ACCOUNTING. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
radaccountsession	<String>	Read-write	Account Session ID to be used in Account Request Packet. Applicable to monitors of type RADIUS_ACCOUNTING. Minimum length = 1
lrtm	<String>	Read-write	Calculate the least response times for bound services. If this parameter is not enabled, the appliance does not learn the response times of the bound services. Also used for LRTM load balancing. Possible values = ENABLED, DISABLED
deviation	<Integer>	Read-write	Time value added to the learned average response time in dynamic response time monitoring (DRTM). When a deviation is specified, the appliance learns the average response time of bound services and adds the deviation to the average. The final value is then continually adjusted

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			to accommodate response time variations over time. Specified in milliseconds, seconds, or minutes. Minimum value = 0 Maximum value = 20939
units1	<String>	Read-write	Unit of measurement for the Deviation parameter. Cannot be changed after the monitor is created. Default value: SEC Possible values = SEC, MSEC, MIN
interval	<Integer>	Read-write	Time interval between two successive probes. Must be greater than the value of Response Time-out. Default value: 5 Minimum value = 1 Maximum value = 20940
units3	<String>	Read-write	monitor interval units. Default value: SEC Possible values = SEC, MSEC, MIN

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
resptimeout	<Integer>	Read-write	Amount of time for which the appliance must wait before it marks a probe as FAILED. Must be less than the value specified for the Interval parameter. Note: For UDP-ECV monitors for which a receive string is not configured, response timeout does not apply. For UDP-ECV monitors with no receive string, probe failure is indicated by an ICMP port unreachable error received from the service. Default value: 2 Minimum value = 1 Maximum value = 20939
units4	<String>	Read-write	monitor response timeout units. Default value: SEC Possible values = SEC, MSEC, MIN
resptimeoutthresh	<Integer>	Read-write	Response time threshold, specified

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			as a percentage of the Response Time-out parameter. If the response to a monitor probe has not arrived when the threshold is reached, the appliance generates an SNMP trap called monRespTimeoutAboveThresh. After the response time returns to a value below the threshold, the appliance generates a monRespTimeoutBelowThresh SNMP trap. For the traps to be generated, the "MONITOR-RTO-THRESHOLD" alarm must also be enabled. Minimum value = 0 Maximum value = 100
retries	<Integer>	Read-write	Maximum number of probes to send to establish the state of a service for which a monitoring probe failed. Default value: 3 Minimum value = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum value = 127
failureretries	<Integer>	Read-write	Number of retries that must fail, out of the number specified for the Retries parameter, for a service to be marked as DOWN. For example, if the Retries parameter is set to 10 and the Failure Retries parameter is set to 6, out of the ten probes sent, at least six probes must fail if the service is to be marked as DOWN. The default value of 0 means that all the retries must fail if the service is to be marked as DOWN. Minimum value = 0 Maximum value = 32
alertretries	<Integer>	Read-write	Number of consecutive probe failures after which the appliance generates an SNMP trap called monProbeFailed. Minimum value = 0

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum value = 32
successretries	<Integer>	Read-write	Number of consecutive successful probes required to transition a service's state from DOWN to UP. Default value: 1 Minimum value = 1 Maximum value = 32
downtime	<Integer>	Read-write	Time duration for which to wait before probing a service that has been marked as DOWN. Expressed in milliseconds, seconds, or minutes. Default value: 30 Minimum value = 1 Maximum value = 20939
units2	<String>	Read-write	Unit of measurement for the Down Time parameter. Cannot be changed after the monitor is created. Default value: SEC Possible values = SEC, MSEC, MIN

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
destip	<String>	Read-write	IP address of the service to which to send probes. If the parameter is set to 0, the IP address of the server to which the monitor is bound is considered the destination IP address.
destport	<Integer>	Read-write	TCP or UDP port to which to send the probe. If the parameter is set to 0, the port number of the service to which the monitor is bound is considered the destination port. For a monitor of type USER, however, the destination port is the port number that is included in the HTTP request sent to the dispatcher. Does not apply to monitors of type PING.
state	<String>	Read-write	State of the monitor. The DISABLED setting disables not only the monitor being configured, but all monitors of the same type, until the parameter is set to ENABLED. If the monitor is bound to a

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			service, the state of the monitor is not taken into account when the state of the service is determined. Default value: ENABLED Possible values = ENABLED, DISABLED
reverse	<String>	Read-write	Mark a service as DOWN, instead of UP, when probe criteria are satisfied, and as UP instead of DOWN when probe criteria are not satisfied. Default value: NO Possible values = YES, NO
transparent	<String>	Read-write	The monitor is bound to a transparent device such as a firewall or router. The state of a transparent device depends on the responsiveness of the services behind it. If a transparent device is being monitored, a destination IP address must be specified. The probe is sent to the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			specified IP address by using the MAC address of the transparent device. Default value: NO Possible values = YES, NO
iptunnel	<String>	Read-write	Send the monitoring probe to the service through an IP tunnel. A destination IP address must be specified. Default value: NO Possible values = YES, NO
tos	<String>	Read-write	Probe the service by encoding the destination IP address in the IP TOS (6) bits. Possible values = YES, NO
tosid	<Integer>	Read-write	The TOS ID of the specified destination IP. Applicable only when the TOS parameter is set. Minimum value = 1 Maximum value = 63
secure	<String>	Read-write	Use a secure SSL connection when monitoring a service.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Applicable only to TCP based monitors. The secure option cannot be used with a CITRIX-AG monitor, because a CITRIX-AG monitor uses a secure connection by default. Default value: NO Possible values = YES, NO
validatecred	<String>	Read-write	Validate the credentials of the Xen Desktop DDC server user. Applicable to monitors of type CITRIX-XD-DDC. Default value: NO Possible values = YES, NO
domain	<String>	Read-write	Domain in which the XenDesktop Desktop Delivery Controller (DDC) servers or Web Interface servers are present. Required by CITRIX-XD-DDC and CITRIX-WI-EXTENDED monitors for logging on to the DDC servers and Web

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Interface servers, respectively.
ipaddress	<String[]>	Read-write	Set of IP addresses expected in the monitoring response from the DNS server, if the record type is A or AAAA. Applicable to DNS monitors. Minimum length = 1
group	<String>	Read-write	Name of a newsgroup available on the NNTP service that is to be monitored. The appliance periodically generates an NNTP query for the name of the newsgroup and evaluates the response. If the newsgroup is found on the server, the service is marked as UP. If the newsgroup does not exist or if the search fails, the service is marked as DOWN. Applicable to NNTP monitors. Minimum length = 1
filename	<String>	Read-write	Name of a file on the FTP server. The appliance monitors the FTP service by periodically checking the existence of the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			file on the server. Applicable to FTP-EXTENDED monitors. Minimum length = 1
basedn	<String>	Read-write	The base distinguished name of the LDAP service, from where the LDAP server can begin the search for the attributes in the monitoring query. Required for LDAP service monitoring. Minimum length = 1
binddn	<String>	Read-write	The distinguished name with which an LDAP monitor can perform the Bind operation on the LDAP server. Optional. Applicable to LDAP monitors. Minimum length = 1
filter	<String>	Read-write	Filter criteria for the LDAP query. Optional. Minimum length = 1
attribute	<String>	Read-write	Attribute to evaluate when the LDAP server responds to the query. Success or failure of the monitoring probe depends on whether the attribute exists in

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			the response. Optional. Minimum length = 1
database	<String>	Read-write	Name of the database to connect to during authentication. Minimum length = 1
oraclesid	<String>	Read-write	Name of the service identifier that is used to connect to the Oracle database during authentication. Minimum length = 1
sqlquery	<String>	Read-write	SQL query for a MYSQL-ECV or MSSQL-ECV monitor. Sent to the database server after the server authenticates the connection. Minimum length = 1
evalrule	<String>	Read-write	Expression that evaluates the database server's response to a MYSQL-ECV or MSSQL-ECV monitoring query. Must produce a Boolean result. The result determines the state of the server. If the expression

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			returns TRUE, the probe succeeds. For example, if you want the appliance to evaluate the error message to determine the state of the server, use the rule MYSQL.RES.ROW(10) .TEXT_ELEM(2).EQ("MySQL").
mssqlprotocolversion	<String>	Read-write	Version of MSSQL server that is to be monitored. Default value: 70 Possible values = 70, 2000, 2000SP1, 2005, 2008, 2008R2, 2012, 2014
Snmpoid	<String>	Read-write	SNMP OID for SNMP monitors. Minimum length = 1
snmpcommunity	<String>	Read-write	Community name for SNMP monitors. Minimum length = 1
snmpthreshold	<String>	Read-write	Threshold for SNMP monitors. Minimum length = 1
snmpversion	<String>	Read-write	SNMP version to be used for SNMP monitors.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = V1, V2
metrictable	<String>	Read-write	Metric table to which to bind metrics. Minimum length = 1 Maximum length = 99
application	<String>	Read-write	Name of the application used to determine the state of the service. Applicable to monitors of type CITRIX-XML-SERVICE. Minimum length = 1
sitepath	<String>	Read-write	URL of the logon page. For monitors of type CITRIX-WEB-INTERFACE, to monitor a dynamic page under the site path, terminate the site path with a slash (/). Applicable to CITRIX-WEB-INTERFACE, CITRIX-WI-EXTENDED and CITRIX-XDM monitors. Minimum length = 1
storename	<String>	Read-write	Store Name. For monitors of type STOREFRONT, STORENAME is an

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			optional argument defining storefront service store name. Applicable to STOREFRONT monitors. Minimum length = 1
storefrontacctservice	<String>	Read-write	Enable/Disable probing for Account Service. Applicable only to Store Front monitors. For multi-tenancy configuration users my skip account service. Default value: YES Possible values = YES, NO
hostname	<String>	Read-write	Hostname in the FQDN format (Example: porche.cars.org). Applicable to STOREFRONT monitors. Minimum length = 1
netprofile	<String>	Read-write	Name of the network profile. Minimum length = 1 Maximum length = 127
originhost	<String>	Read-write	Origin-Host value for the Capabilities-Exchange-Request

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			(CER) message to use for monitoring Diameter servers. Minimum length = 1
originrealm	<String>	Read-write	Origin-Realm value for the Capabilities-Exchange-Request (CER) message to use for monitoring Diameter servers. Minimum length = 1
hostipaddress	<String>	Read-write	Host-IP-Address value for the Capabilities-Exchange-Request (CER) message to use for monitoring Diameter servers. If Host-IP-Address is not specified, the appliance inserts the mapped IP (MIP) address or subnet IP (SNIP) address from which the CER request (the monitoring probe) is sent. Minimum length = 1
vendorid	<Integer>	Read-write	Vendor-Id value for the Capabilities-Exchange-Request (CER) message to use for monitoring Diameter servers.
productname	<String>	Read-write	Product-Name value for the Capabilities-

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Exchange-Request (CER) message to use for monitoring Diameter servers. Minimum length = 1
firmwarerevision	<Integer>	Read-write	Firmware-Revision value for the Capabilities-Exchange-Request (CER) message to use for monitoring Diameter servers.
authapplicationid	<Integer[]>	Read-write	List of Auth-Application-Id attribute value pairs (AVPs) for the Capabilities-Exchange-Request (CER) message to use for monitoring Diameter servers. A maximum of eight of these AVPs are supported in a monitoring CER message. Minimum value = 0 Maximum value = 4294967295
acctapplicationid	<Integer[]>	Read-write	List of Acct-Application-Id attribute value pairs (AVPs) for the Capabilities-Exchange-Request (CER) message to use for monitoring

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Diameter servers. A maximum of eight of these AVPs are supported in a monitoring message. Minimum value = 0 Maximum value = 4294967295
inbandsecurityid	<String>	Read-write	Inband-Security-Id for the Capabilities-Exchange-Request (CER) message to use for monitoring Diameter servers. Possible values = NO_INBAND_SECURITY, TLS
supportedvendorids	<Integer[]>	Read-write	List of Supported-Vendor-Id attribute value pairs (AVPs) for the Capabilities-Exchange-Request (CER) message to use for monitoring Diameter servers. A maximum eight of these AVPs are supported in a monitoring message. Minimum value = 1 Maximum value = 4294967295
vendorspecificvendorid	<Integer>	Read-write	Vendor-Id to use in the Vendor-Specific-Application-Id grouped attribute-

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			value pair (AVP) in the monitoring CER message. To specify Auth-Application-Id or Acct-Application-Id in Vendor-Specific-Application-Id, use vendorSpecificAuthApplicationIds or vendorSpecificAcctApplicationIds, respectively. Only one Vendor-Id is supported for all the Vendor-Specific-Application-Id AVPs in a CER monitoring message. Minimum value = 1
vendorspecificauthapplicationids	<Integer[]>	Read-write	List of Vendor-Specific-Auth-Application-Id attribute value pairs (AVPs) for the Capabilities-Exchange-Request (CER) message to use for monitoring Diameter servers. A maximum of eight of these AVPs are supported in a monitoring message. The specified value is combined with the value of vendorSpecificVendorId to obtain the Vendor-Specific-Application-Id AVP in

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			the CER monitoring message. Minimum value = 0 Maximum value = 4294967295
vendorspecificacctapplicationids	<Integer[]>	Read-write	List of Vendor-Specific-Acct-Application-Id attribute value pairs (AVPs) to use for monitoring Diameter servers. A maximum of eight of these AVPs are supported in a monitoring message. The specified value is combined with the value of vendorSpecificVendorId to obtain the Vendor-Specific-Application-Id AVP in the CER monitoring message. Minimum value = 0 Maximum value = 4294967295
kcdaccount	<String>	Read-write	KCD Account used by MSSQL monitor. Minimum length = 1 Maximum length = 32
storedb	<String>	Read-write	Store the database list populated with

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			the responses to monitor probes. Used in database specific load balancing if MSSQL-ECV/MYSQL-ECV monitor is configured. Default value: DISABLED Possible values = ENABLED, DISABLED
storefrontcheckbackendservices	<String>	Read-write	This option will enable monitoring of services running on storefront server. Storefront services are monitored by probing to a Windows service that runs on the Storefront server and exposes details of which storefront services are running. Default value: NO Possible values = YES, NO
trofscode	<Integer>	Read-write	Code expected when the server is under maintenance.
trofsstring	<String>	Read-write	String expected from the server for the service to be marked as trofs. Applicable

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			to HTTP-ECV/TCP-ECV monitors.
sslprofile	<String>	Read-write	SSL Profile associated with the monitor. Minimum length = 1 Maximum length = 127
mqttclientidentifier	<String>	Read-write	Client id to be used in Connect command.
mqttversion	<Integer>	Read-write	Version of MQTT protocol used in connect message, default is version 3.1.1 [4]. Default value: 4 Minimum value = 3
grpchealthcheck	<String>	Read-write	Option to enable or disable gRPC health check service. Default value: NO Possible values = YES, NO
grpcstatuscode	<Integer[]>	Read-write	gRPC status codes for which to mark the service as UP. The default value is 12(health check unimplemented). If the gRPC status code 0 is received from the backend

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			this configuration is ignored.
grpcservicename	<String>	Read-write	Option to specify gRPC service name on which gRPC health check need to be performed.
metric	<String>	Read-write	Metric name in the metric table, whose setting is changed. A value zero disables the metric and it will not be used for load calculation. Minimum length = 1 Maximum length = 37
metricthreshold	<Integer>	Read-write	Threshold to be used for that metric.
metricweight	<Integer>	Read-write	The weight for the specified service metric with respect to others. Minimum value = 1 Maximum value = 100
servicename	<String>	Read-write	The name of the service to which the monitor is bound. Minimum length = 1
servicegroupname	<String>	Read-write	The name of the service group to

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			which the monitor is to be bound. Minimum length = 1
lrtmconf	<Integer>	Read-only	State of LRTM configuration on the monitor.
lrtmconfstr	<String>	Read-only	State of LRTM configuration on the monitor as STRING. Possible values = ENABLED, DISABLED
dynamicresponsetimeout	<Integer>	Read-only	Response timeout of the DRTM enabled monitor , calculated dynamically based on the history and current response time.
dynamicinterval	<Integer>	Read-only	Interval between monitoring probes for DRTM enabled monitor , calculated dynamically based monitor response time.
multimetrictable	<String[]>	Read-only	Metric table to which to bind metrics, to be used only for output purposes.
dup_state	<String>	Read-only	. Default value: ENABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ENABLED, DISABLED
dup_weight	<Integer>	Read-only	. Default value: 1 Minimum value = 1 Maximum value = 100
weight	<Integer>	Read-only	. Minimum value = 1 Maximum value = 100
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- ENABLE
- DISABLE
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbmonitor **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"lbmonitor":{

<b>"monitorname":<String_value>,

</b><b>"type":<String_value>,

</b>"action":<String_value>,
```

```
"respcode":<String[]_value>,

"httprequest":<String_value>,

"rtsprequest":<String_value>,

"customheaders":<String_value>,

"maxforwards":<Integer_value>,

"sipmethod":<String_value>,

"sipuri":<String_value>,

"sipreguri":<String_value>,

"send":<String_value>,

"recv":<String_value>,

"query":<String_value>,

"querytype":<String_value>,

"scriptname":<String_value>,

"scriptargs":<String_value>,

"secureargs":<String_value>,

"dispatcherip":<String_value>,

"dispatcherport":<Integer_value>,

"username":<String_value>,

"password":<String_value>,

"secondarypassword":<String_value>,

"logonpointname":<String_value>,

"lasversion":<String_value>,
```

```
"radkey":<String_value>,

"radnasid":<String_value>,

"radnasip":<String_value>,

"radaccounttype":<Integer_value>,

"radframedip":<String_value>,

"radapn":<String_value>,

"radmsisdn":<String_value>,

"radaccountsession":<String_value>,

"lrtm":<String_value>,

"deviation":<Integer_value>,

"units1":<String_value>,

"interval":<Integer_value>,

"units3":<String_value>,

"resptimeout":<Integer_value>,

"units4":<String_value>,

"resptimeoutthresh":<Integer_value>,

"retries":<Integer_value>,

"failureretries":<Integer_value>,

"alertretries":<Integer_value>,

"successretries":<Integer_value>,

"downtime":<Integer_value>,

"units2":<String_value>,
```

```
"destip":<String_value>,

"destport":<Integer_value>,

"state":<String_value>,

"reverse":<String_value>,

"transparent":<String_value>,

"iptunnel":<String_value>,

"tos":<String_value>,

"tosid":<Integer_value>,

"secure":<String_value>,

"validatecred":<String_value>,

"domain":<String_value>,

"ipaddress":<String[]_value>,

"group":<String_value>,

"filename":<String_value>,

"basedn":<String_value>,

"binddn":<String_value>,

"filter":<String_value>,

"attribute":<String_value>,

"database":<String_value>,

"oraclesid":<String_value>,

"sqlquery":<String_value>,

"evalrule":<String_value>,
```

```
"mssqlprotocolversion":<String_value>,

"Snmpoid":<String_value>,

"snmpcommunity":<String_value>,

"snmpthreshold":<String_value>,

"snmpversion":<String_value>,

"metrictable":<String_value>,

"application":<String_value>,

"sitepath":<String_value>,

"storename":<String_value>,

"storefrontacctservice":<String_value>,

"hostname":<String_value>,

"netprofile":<String_value>,

"originhost":<String_value>,

"originrealm":<String_value>,

"hostipaddress":<String_value>,

"vendorid":<Integer_value>,

"productname":<String_value>,

"firmwarerevision":<Integer_value>,

"authapplicationid":<Integer[]_value>,

"acctapplicationid":<Integer[]_value>,

"inbandsecurityid":<String_value>,

"supportedvendorids":<Integer[]_value>,
```

```
"vendorspecificvendorid":<Integer_value>,

"vendorspecificauthapplicationids":<Integer[]_value>,

"vendorspecificacctapplicationids":<Integer[]_value>,

"kcdaccount":<String_value>,

"storedb":<String_value>,

"storefrontcheckbackendservices":<String_value>,

"trofscode":<Integer_value>,

"trofsstring":<String_value>,

"sslprofile":<String_value>,

"mqttclientidentifier":<String_value>,

"mqttversion":<Integer_value>,

"grpchealthcheck":<String_value>,

"grpcstatuscode":<Integer[]_value>,

"grpcservicename":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbmonitor/ monitorname_value<String> **Query-parameters: args= type:<String_value>, respcode: <String_value>**

update

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbmonitor **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"lbmonitor":{

<b>"monitorname":<String_value>,

</b><b>"type":<String_value>,

</b>"action":<String_value>,

"respcode":<String[]_value>,

"httprequest":<String_value>,

"rtsprequest":<String_value>,

"customheaders":<String_value>,

"maxforwards":<Integer_value>,

"sipmethod":<String_value>,

"sipreguri":<String_value>,

"sipuri":<String_value>,

"send":<String_value>,

"recv":<String_value>,

"query":<String_value>,

"querytype":<String_value>,

"username":<String_value>,

"password":<String_value>,
```

```
"secondarypassword":<String_value>,

"logonpointname":<String_value>,

"lasversion":<String_value>,

"radkey":<String_value>,

"radnasid":<String_value>,

"radnasip":<String_value>,

"radaccounttype":<Integer_value>,

"radframedip":<String_value>,

"radapn":<String_value>,

"radmsisdn":<String_value>,

"radaccountsession":<String_value>,

"lrtm":<String_value>,

"deviation":<Integer_value>,

"units1":<String_value>,

"scriptname":<String_value>,

"scriptargs":<String_value>,

"secureargs":<String_value>,

"validatecred":<String_value>,

"domain":<String_value>,

"dispatcherip":<String_value>,

"dispatcherport":<Integer_value>,

"interval":<Integer_value>,
```

```
"units3":<String_value>,

"resptimeout":<Integer_value>,

"units4":<String_value>,

"resptimeoutthresh":<Integer_value>,

"retries":<Integer_value>,

"failureretries":<Integer_value>,

"alertretries":<Integer_value>,

"successretries":<Integer_value>,

"downtime":<Integer_value>,

"units2":<String_value>,

"destip":<String_value>,

"destport":<Integer_value>,

"state":<String_value>,

"reverse":<String_value>,

"transparent":<String_value>,

"iptunnel":<String_value>,

"tos":<String_value>,

"tosid":<Integer_value>,

"secure":<String_value>,

"ipaddress":<String[]_value>,

"group":<String_value>,

"filename":<String_value>,
```

```
"basedn":<String_value>,

"binddn":<String_value>,

"filter":<String_value>,

"attribute":<String_value>,

"database":<String_value>,

"oraclesid":<String_value>,

"sqlquery":<String_value>,

"evalrule":<String_value>,

"Snmpoid":<String_value>,

"snmpcommunity":<String_value>,

"snmpthreshold":<String_value>,

"snmpversion":<String_value>,

"metrictable":<String_value>,

"metric":<String_value>,

"metricthreshold":<Integer_value>,

"metricweight":<Integer_value>,

"application":<String_value>,

"sitepath":<String_value>,

"storename":<String_value>,

"storefrontacctservice":<String_value>,

"storefrontcheckbackendservices":<String_value>,

"hostname":<String_value>,
```

```
"netprofile":<String_value>,

"mssqlprotocolversion":<String_value>,

"originhost":<String_value>,

"originrealm":<String_value>,

"hostipaddress":<String_value>,

"vendorid":<Integer_value>,

"productname":<String_value>,

"firmwarerevision":<Integer_value>,

"authapplicationid":<Integer[]_value>,

"acctapplicationid":<Integer[]_value>,

"inbandsecurityid":<String_value>,

"supportedvendorids":<Integer[]_value>,

"vendorspecificvendorid":<Integer_value>,

"vendorspecificauthapplicationids":<Integer[]_value>,

"vendorspecificacctapplicationids":<Integer[]_value>,

"kcdaccount":<String_value>,

"storedb":<String_value>,

"trofscode":<Integer_value>,

"trofsstring":<String_value>,

"sslprofile":<String_value>,

"mqttclientidentifier":<String_value>,

"mqttversion":<Integer_value>,
```

```
"grpchealthcheck":<String_value>,

"grpcstatuscode":<Integer[]_value>,

"grpcservicename":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

unset

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbmonitor? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"lbmonitor":{

<b>"monitorname":<String_value>,

</b><b>"type":<String_value>,

</b>"ipaddress":true,

"scriptname":true,

"destport":true,

"netprofile":true,

"sslprofile":true,

"action":true,
```

```
"respcode":true,

"httprequest":true,

"rtsprequest":true,

"customheaders":true,

"maxforwards":true,

"sipmethod":true,

"sipreguri":true,

"send":true,

"recv":true,

"query":true,

"querytype":true,

"username":true,

"password":true,

"secondarypassword":true,

"logonpointname":true,

"lasversion":true,

"radkey":true,

"radnasid":true,

"radnasip":true,

"radaccounttype":true,

"radframedip":true,

"radapn":true,
```

```
"radmsisdn":true,

"radaccountsession":true,

"lrtm":true,

"deviation":true,

"scriptargs":true,

"secureargs":true,

"validatecred":true,

"domain":true,

"dispatcherip":true,

"dispatcherport":true,

"interval":true,

"resptimeout":true,

"resptimeoutthresh":true,

"retries":true,

"failureretries":true,

"alertretries":true,

"successretries":true,

"downtime":true,

"destip":true,

"state":true,

"reverse":true,

"transparent":true,
```

```
"iptunnel":true,

"tos":true,

"tosid":true,

"secure":true,

"group":true,

"filename":true,

"basedn":true,

"binddn":true,

"filter":true,

"attribute":true,

"database":true,

"oraclesid":true,

"sqlquery":true,

"Snmpoid":true,

"snmpcommunity":true,

"snmpthreshold":true,

"snmpversion":true,

"metrictable":true,

"mssqlprotocolversion":true,

"originhost":true,

"originrealm":true,

"hostipaddress":true,
```

```
"vendorid":true,

"productname":true,

"firmwarerevision":true,

"authapplicationid":true,

"acctapplicationid":true,

"inbandsecurityid":true,

"supportedvendorids":true,

"vendorspecificvendorid":true,

"vendorspecificauthapplicationids":true,

"vendorspecificacctapplicationids":true,

"kcdaccount":true,

"storedb":true,

"trofscode":true,

"trofsstring":true,

"mqttclientidentifier":true,

"mqttversion":true,

"grpchealthcheck":true,

"grpcstatuscode":true,

"grpcservicename":true

}}
```


Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

enable

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbmonitor? **action=enable HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"lbmonitor":{

"servicename":<String_value>,

"servicegroupname":<String_value>,

"monitorname":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

disable

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbmonitor? **action=disable HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"lbmonitor":{

"servicename":<String_value>,

"servicegroupname":<String_value>,

"monitorname":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error
get (all)
URL: http:// <netscaler-ip-address> /nitro/v1/config/lbmonitor **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/lbmonitor? **args=monitorname: <String_value> ,type: <String_value>**

Use this query-parameter to get lbmonitor resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/config/lbmonitor? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/lbmonitor? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of lbmonitor resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/lbmonitor? **view=summary**

Use this query-parameter to get the summary output of lbmonitor resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/lbmonitor? **pagesize=#no;pageno=#no**

Use this query-parameter to get the lbmonitor resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "lbmonitor": [ {

monitorname:<String_value>,type:<String_value>"interval":<Integer_value>,

"units3":<String_value>,

"resptimeout":<Integer_value>,

"resptimeoutthresh":<Integer_value>,

"units4":<String_value>,

"retries":<Integer_value>,

"failureretries":<Integer_value>,

"alertretries":<Integer_value>,

"successretries":<Integer_value>,

"downtime":<Integer_value>,

"units2":<String_value>,

"destip":<String_value>,
```

```
"destport":<Integer_value>,

"state":<String_value>,

"reverse":<String_value>,

"transparent":<String_value>,

"iptunnel":<String_value>,

"tos":<String_value>,

"tosid":<Integer_value>,

"secure":<String_value>,

"action":<String_value>,

"respcode":<String[]_value>,

"httprequest":<String_value>,

"rtsprequest":<String_value>,

"send":<String_value>,

"recv":<String_value>,

"query":<String_value>,

"querytype":<String_value>,

"username":<String_value>,

"password":<String_value>,

"secondarypassword":<String_value>,

"logonpointname":<String_value>,

"lasversion":<String_value>,

"validatecred":<String_value>,
```

```
"domain":<String_value>,

"radkey":<String_value>,

"radnasid":<String_value>,

"radnasip":<String_value>,

"radaccounttype":<Integer_value>,

"radframedip":<String_value>,

"radapn":<String_value>,

"radmsisdn":<String_value>,

"radaccountsession":<String_value>,

"lrtm":<String_value>,

"lrtmconf":<Integer_value>,

"lrtmconfstr":<String_value>,

"deviation":<Integer_value>,

"units1":<String_value>,

"dynamicresponsetimeout":<Integer_value>,

"dynamicinterval":<Integer_value>,

"scriptname":<String_value>,

"scriptargs":<String_value>,

"secureargs":<String_value>,

"dispatcherip":<String_value>,

"dispatcherport":<Integer_value>,

"sipuri":<String_value>,
```

```
"sipmethod":<String_value>,

"maxforwards":<Integer_value>,

"sipreguri":<String_value>,

"customheaders":<String_value>,

"ipaddress":<String[]_value>,

"group":<String_value>,

"filename":<String_value>,

"basedn":<String_value>,

"binddn":<String_value>,

"filter":<String_value>,

"attribute":<String_value>,

"database":<String_value>,

"oraclesid":<String_value>,

"sqlquery":<String_value>,

"evalrule":<String_value>,

"Snmpoid":<String_value>,

"snmpcommunity":<String_value>,

"snmpthreshold":<String_value>,

"snmpversion":<String_value>,

"metric":<String_value>,

"metrictable":<String_value>,

"multimetrictable":<String[]_value>,
```

```
"metricthreshold":<Integer_value>,

"metricweight":<Integer_value>,

"application":<String_value>,

"sitepath":<String_value>,

"storename":<String_value>,

"storefrontacctservice":<String_value>,

"storefrontcheckbackendservices":<String_value>,

"hostname":<String_value>,

"netprofile":<String_value>,

"mssqlprotocolversion":<String_value>,

"originhost":<String_value>,

"originrealm":<String_value>,

"hostipaddress":<String_value>,

"vendorid":<Integer_value>,

"productname":<String_value>,

"firmwarerevision":<Integer_value>,

"authapplicationid":<Integer[]_value>,

"acctapplicationid":<Integer[]_value>,

"inbandsecurityid":<String_value>,

"supportedvendorids":<Integer[]_value>,

"vendorspecificvendorid":<Integer_value>,

"vendorspecificauthapplicationids":<Integer[]_value>,
```

```
"vendorspecificacctapplicationids":<Integer[]_value>,

"servicename":<String_value>,

"dup_state":<String_value>,

"dup_weight":<Integer_value>,

"servicegroupname":<String_value>,

"weight":<Integer_value>,

"kcdaccount":<String_value>,

"storedb":<String_value>,

"trofscode":<Integer_value>,

"trofsstring":<String_value>,

"sslprofile":<String_value>,

"mqttclientidentifier":<String_value>,

"mqttversion":<Integer_value>,

"grpchealthcheck":<String_value>,

"grpcstatuscode":<Integer[]_value>,

"grpcservicename":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

get

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbmonitor/ monitorname_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/lbmonitor/ monitorname_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/lbmonitor/ monitorname_value<String> ? **view=summary**

Use this query-parameter to get the summary output of lbmonitor resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lbmonitor": [ {

monitorname:<String_value>,type:<String_value>"interval":<Integer_value>,

"units3":<String_value>,

"resptimeout":<Integer_value>,

"resptimeoutthresh":<Integer_value>,

"units4":<String_value>,

"retries":<Integer_value>,

"failureretries":<Integer_value>,
```

```
"alertretries":<Integer_value>,

"successretries":<Integer_value>,

"downtime":<Integer_value>,

"units2":<String_value>,

"destip":<String_value>,

"destport":<Integer_value>,

"state":<String_value>,

"reverse":<String_value>,

"transparent":<String_value>,

"iptunnel":<String_value>,

"tos":<String_value>,

"tosid":<Integer_value>,

"secure":<String_value>,

"action":<String_value>,

"respcode":<String[]_value>,

"httprequest":<String_value>,

"rtsprequest":<String_value>,

"send":<String_value>,

"recv":<String_value>,

"query":<String_value>,

"querytype":<String_value>,

"username":<String_value>,
```

```
"password":<String_value>,

"secondarypassword":<String_value>,

"logonpointname":<String_value>,

"lasversion":<String_value>,

"validatecred":<String_value>,

"domain":<String_value>,

"radkey":<String_value>,

"radnasid":<String_value>,

"radnasip":<String_value>,

"radaccounttype":<Integer_value>,

"radframedip":<String_value>,

"radapn":<String_value>,

"radmsisdn":<String_value>,

"radaccountsession":<String_value>,

"lrtm":<String_value>,

"lrtmconf":<Integer_value>,

"lrtmconfstr":<String_value>,

"deviation":<Integer_value>,

"units1":<String_value>,

"dynamicresponsetimeout":<Integer_value>,

"dynamicinterval":<Integer_value>,

"scriptname":<String_value>,
```

```
"scriptargs":<String_value>,

"secureargs":<String_value>,

"dispatcherip":<String_value>,

"dispatcherport":<Integer_value>,

"sipuri":<String_value>,

"sipmethod":<String_value>,

"maxforwards":<Integer_value>,

"sipreguri":<String_value>,

"customheaders":<String_value>,

"ipaddress":<String[]_value>,

"group":<String_value>,

"filename":<String_value>,

"basedn":<String_value>,

"binddn":<String_value>,

"filter":<String_value>,

"attribute":<String_value>,

"database":<String_value>,

"oraclesid":<String_value>,

"sqlquery":<String_value>,

"evalrule":<String_value>,

"Snmpoid":<String_value>,

"snmpcommunity":<String_value>,
```

```
"snmpthreshold":<String_value>,

"snmpversion":<String_value>,

"metric":<String_value>,

"metrictable":<String_value>,

"multimetrictable":<String[]_value>,

"metricthreshold":<Integer_value>,

"metricweight":<Integer_value>,

"application":<String_value>,

"sitepath":<String_value>,

"storename":<String_value>,

"storefrontacctservice":<String_value>,

"storefrontcheckbackendservices":<String_value>,

"hostname":<String_value>,

"netprofile":<String_value>,

"mssqlprotocolversion":<String_value>,

"originhost":<String_value>,

"originrealm":<String_value>,

"hostipaddress":<String_value>,

"vendorid":<Integer_value>,

"productname":<String_value>,

"firmwarerevision":<Integer_value>,

"authapplicationid":<Integer[]_value>,
```

```
"acctapplicationid":<Integer[]_value>,

"inbandsecurityid":<String_value>,

"supportedvendorids":<Integer[]_value>,

"vendorspecificvendorid":<Integer_value>,

"vendorspecificauthapplicationids":<Integer[]_value>,

"vendorspecificacctapplicationids":<Integer[]_value>,

"servicename":<String_value>,

"dup_state":<String_value>,

"dup_weight":<Integer_value>,

"servicegroupname":<String_value>,

"weight":<Integer_value>,

"kcdaccount":<String_value>,

"storedb":<String_value>,

"trofscode":<Integer_value>,

"trofsstring":<String_value>,

"sslprofile":<String_value>,

"mqttclientidentifier":<String_value>,

"mqttversion":<Integer_value>,

"grpchealthcheck":<String_value>,

"grpcstatuscode":<Integer[]_value>,

"grpcservicename":<String_value>,

"_nextgenapiresource":<String_value>
```

```
}]}
```

count

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbmonitor? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "lbmonitor": [ { "__count": "#no"} ] }
```

lbmonitor_binding

Binding object which returns the resources bound to lbmonitor.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
monitorname	<String>	Read-write	Name of the monitor. Minimum length = 1
lbmonitor_sslcertkey_binding	<lbmonitor_sslcertkey_binding[]>	Read-only	sslcertkey that can be bound to lbmonitor.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
lbmonitor_metric_binding	<lbmonitor_metric_binding[]>	Read-only	metric that can be bound to lbmonitor.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbmonitor_binding/ monitorname_value<String>
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "lbmonitor_binding": [ {

"monitorname":<String_value>,

"lbmonitor_sslcertkey_binding":<lbmonitor_sslcertkey_binding[]_value>,

"lbmonitor_metric_binding":<lbmonitor_metric_binding[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbmonitor_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/lbmonitor_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "lbmonitor_binding": [ {

"monitorname":<String_value>,

"lbmonitor_sslcertkey_binding":<lbmonitor_sslcertkey_binding[]_value>,

"lbmonitor_metric_binding":<lbmonitor_metric_binding[]_value>

}]}
```

lbmonitor_metric_binding

Binding object showing the metric that can be bound to lbmonitor.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
metric	<String>	Read-write	Metric name in the metric table, whose setting is changed. A value zero disables the metric and it will not be used for load calculation. Minimum length = 1 Maximum length = 37

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
metricthreshold	<Integer>	Read-write	Threshold to be used for that metric.
metricweight	<Integer>	Read-write	The weight for the specified service metric with respect to others. Minimum value = 1 Maximum value = 100
monitorname	<String>	Read-write	Name of the monitor. Minimum length = 1
metric_unit	<String>	Read-only	Giving the unit of the metric. Possible values = Bytes/s, ms, pkts/s, users
metrictable	<String>	Read-only	Metric table to which to bind metrics. Minimum length = 1 Maximum length = 99
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/lbmonitor_metric_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"lbmonitor_metric_binding":{

<b>"monitorname":<String_value>,
```

```
</b>"metric":<String_value>,

"metricthreshold":<Integer_value>,

"metricweight":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbmonitor_metric_binding/ monitorname_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/ config/lbmonitor_metric_binding/ monitorname_value<String> ? **args=metric: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbmonitor_metric_binding/ monitorname_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/ config/lbmonitor_metric_binding/ monitorname_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of lbmonitor_metric_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/lbmonitor_metric_binding/ monitorname_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the lbmonitor_metric_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lbmonitor_metric_binding": [ {

"metric":<String_value>,

"metricthreshold":<Integer_value>,

"metricweight":<Integer_value>,

"monitorname":<String_value>,

"metric_unit":<String_value>,

"metrictable":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbmonitor_metric_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/lbmonitor_metric_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lbmonitor_metric_binding": [ {

"metric":<String_value>,

"metricthreshold":<Integer_value>,

"metricweight":<Integer_value>,

"monitorname":<String_value>,

"metric_unit":<String_value>,

"metrictable":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbmonitor_metric_binding/monitorname_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"lbmonitor_metric_binding": [ { "__count": "#no"} ] }
```

lbmonitor_service_binding

Binding object showing the service that can be bound to lbmonitor.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
servicename	<String>	Read-write	Name of the service or service group. Minimum length = 1
monitorname	<String>	Read-write	Name of the monitor. Minimum length = 1
dup_weight	<Integer>	Read-write	Weight to assign to the binding between the monitor and service. Default value: 1 Minimum value = 1 Maximum value = 100

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
dup_state	<String>	Read-write	State of the monitor. The state setting for a monitor of a given type affects all monitors of that type. For example, if an HTTP monitor is enabled, all HTTP monitors on the appliance are (or remain) enabled. If an HTTP monitor is disabled, all HTTP monitors on the appliance are disabled. Default value: ENABLED Possible values = ENABLED, DISABLED
servicegroupname	<String>	Read-write	Name of the service group. Minimum length = 1
weight	<Integer>	Read-write	Weight to assign to the binding between the monitor and service. Minimum value = 1 Maximum value = 100
state	<String>	Read-write	State of the monitor. The state setting for a monitor of a given type affects all

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			monitors of that type. For example, if an HTTP monitor is enabled, all HTTP monitors on the appliance are (or remain) enabled. If an HTTP monitor is disabled, all HTTP monitors on the appliance are disabled. Default value: ENABLED Possible values = ENABLED, DISABLED

Operations

(click to see Properties)

- ADD
- DELETE

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of

creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/lbmonitor_service_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"lbmonitor_service_binding":{

<b>"monitorname":<String_value>,

</b>"servicename":<String_value>,

"dup_state":<String_value>,

"dup_weight":<Integer_value>,

"servicegroupname":<String_value>,

"state":<String_value>,

"weight":<Integer_value>
```

```
}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbmonitor_service_binding/ monitorname_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/ config/lbmonitor_service_binding/ monitorname_value<String> ? **args=servicename: <String_value> ,servicegroupname: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

lbmonitor_servicegroup_binding

Binding object showing the servicegroup that can be bound to lbmonitor.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
state	<String>	Read-write	State of the monitor. The state setting for a monitor of a given type affects all monitors of that type. For example, if an HTTP monitor is enabled, all HTTP

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			monitors on the appliance are (or remain) enabled. If an HTTP monitor is disabled, all HTTP monitors on the appliance are disabled. Default value: ENABLED Possible values = ENABLED, DISABLED
servicegroupname	<String>	Read-write	Name of the service group. Minimum length = 1
weight	<Integer>	Read-write	Weight to assign to the binding between the monitor and service. Minimum value = 1 Maximum value = 100
dup_weight	<Integer>	Read-write	Weight to assign to the binding between the monitor and service. Default value: 1 Minimum value = 1 Maximum value = 100

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
dup_state	<String>	Read-write	State of the monitor. The state setting for a monitor of a given type affects all monitors of that type. For example, if an HTTP monitor is enabled, all HTTP monitors on the appliance are (or remain) enabled. If an HTTP monitor is disabled, all HTTP monitors on the appliance are disabled. Default value: ENABLED Possible values = ENABLED, DISABLED
monitorname	<String>	Read-write	Name of the monitor. Minimum length = 1
servicename	<String>	Read-write	Name of the service or service group. Minimum length = 1

Operations

(click to see Properties)

- ADD
- DELETE

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/lbmonitor_servicegroup_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"lbmonitor_servicegroup_binding":{

<b>"monitorname":<String_value>,
```

```
</b>"servicename":<String_value>,

"dup_state":<String_value>,

"dup_weight":<Integer_value>,

"servicegroupname":<String_value>,

"state":<String_value>,

"weight":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbmonitor_servicegroup_binding/ monitorname_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/ config/lbmonitor_servicegroup_binding/ monitorname_value<String> ? **args=servicename: <String_value> ,servicegroupname: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

lbmonitor_sslcertkey_binding

Binding object showing the sslcertkey that can be bound to lbmonitor.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
crlcheck	<String>	Read-write	The state of the CRL check parameter. (Mandatory/ Optional). Possible values = Mandatory, Optional
ocspcheck	<String>	Read-write	The state of the OCSP check parameter. (Mandatory/ Optional). Possible values = Mandatory, Optional
monitorname	<String>	Read-write	Name of the monitor. Minimum length = 1
certkeyname	<String>	Read-write	The name of the certificate bound to the monitor.
ca	<Boolean>	Read-write	The rule for use of CRL corresponding to this CA certificate during client authentication. If crlCheck is set to Mandatory, the system will deny all SSL clients if the CRL is missing, expired - NextUpdate date is in the past, or is incomplete with remote CRL refresh enabled. If crlCheck is set to optional, the system will allow SSL clients in the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			above error cases.However, in any case if the client certificate is revoked in the CRL, the SSL client will be denied access.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/lbmonitor_sslcertkey_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"lbmonitor_sslcertkey_binding":{

<b>"monitorname":<String_value>,

</b>"certkeyname":<String_value>,

"ca":<Boolean_value>,

"crlcheck":<String_value>,

"ocspcheck":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbmonitor_sslcertkey_binding/ monitorname_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/ config/lbmonitor_sslcertkey_binding/ monitorname_value<String> ? **args=certkeyname: <String_value> ,ca: <Boolean_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbmonitor_sslcertkey_binding/ monitorname_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/ config/lbmonitor_sslcertkey_binding/ monitorname_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of lbmonitor_sslcertkey_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/lbmonitor_sslcertkey_binding/ monitorname_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the lbmonitor_sslcertkey_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lbmonitor_sslcertkey_binding": [ {

"crlcheck":<String_value>,

"ocspcheck":<String_value>,

"monitorname":<String_value>,

"certkeyname":<String_value>,

"ca":<Boolean_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbmonitor_sslcertkey_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/lbmonitor_sslcertkey_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lbmonitor_sslcertkey_binding": [ {

"crlcheck":<String_value>,

"ocspcheck":<String_value>,

"monitorname":<String_value>,

"certkeyname":<String_value>,

"ca":<Boolean_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbmonitor_sslcertkey_binding/ monitorname_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"lbmonitor_sslcertkey_binding": [ { "__count": "#no"} ] }
```

lbparameter

Configuration for LB parameter resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
httponlycookieflag	<String>	Read-write	Include the HttpOnly attribute in persistence cookies. The HttpOnly attribute limits the scope of a cookie to HTTP requests and helps mitigate the risk of cross-site scripting attacks. Default value: ENABLED Possible values = ENABLED, DISABLED
usesecuredpersistencecookie	<String>	Read-write	Encode persistence cookie values using SHA2 hash. Default value: DISABLED Possible values = ENABLED, DISABLED
useencryptedpersistencecookie	<String>	Read-write	Encode persistence cookie values using SHA2 hash. Default value: DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ENABLED, DISABLED
cookiepassphrase	<String>	Read-write	Use this parameter to specify the passphrase used to generate secured persistence cookie value. It specifies the passphrase with a maximum of 31 characters.
consolidatedlconn	<String>	Read-write	To find the service with the fewest connections, the virtual server uses the consolidated connection statistics from all the packet engines. The NO setting allows consideration of only the number of connections on the packet engine that received the new connection. Default value: YES Possible values = YES, NO
useportforhashlb	<String>	Read-write	Include the port number of the service when creating a hash for hash based load balancing methods. With the NO setting,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			only the IP address of the service is considered when creating a hash. Default value: YES Possible values = YES, NO
preferdirectroute	<String>	Read-write	Perform route lookup for traffic received by the Citrix ADC, and forward the traffic according to configured routes. Do not set this parameter if you want a wildcard virtual server to direct packets received by the appliance to an intermediary device, such as a firewall, even if their destination is directly connected to the appliance. Route lookup is performed after the packets have been processed and returned by the intermediary device. Default value: YES Possible values = YES, NO
startuprrfactor	<Integer>	Read-write	Number of requests, per service, for which

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			to apply the round robin load balancing method before switching to the configured load balancing method, thus allowing services to ramp up gradually to full load. Until the specified number of requests is distributed, the Citrix ADC is said to be implementing the slow start mode (or startup round robin). Implemented for a virtual server when one of the following is true: * The virtual server is newly created. * One or more services are newly bound to the virtual server. * One or more services bound to the virtual server are enabled. * The load balancing method is changed. This parameter applies to all the load balancing

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			virtual servers configured on the Citrix ADC, except for those virtual servers for which the virtual server-level slow start parameters (New Service Startup Request Rate and Increment Interval) are configured. If the global slow start parameter and the slow start parameters for a given virtual server are not set, the appliance implements a default slow start for the virtual server, as follows: * For a newly configured virtual server, the appliance implements slow start for the first 100 requests received by the virtual server. * For an existing virtual server, if one or more services are newly bound or

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			newly enabled, or if the load balancing method is changed, the appliance dynamically computes the number of requests for which to implement startup round robin. It obtains this number by multiplying the request rate by the number of bound services (it includes services that are marked as DOWN). For example, if the current request rate is 20 requests/s and ten services are bound to the virtual server, the appliance performs startup round robin for 200 requests. Not applicable to a virtual server for which a hash based load balancing method is configured.
monitorskipmaxclient	<String>	Read-write	When a monitor initiates a connection to a service, do not

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			check to determine whether the number of connections to the service has reached the limit specified by the service's Max Clients setting. Enables monitoring to continue even if the service has reached its connection limit. Default value: DISABLED Possible values = ENABLED, DISABLED
monitorconnectionclose	<String>	Read-write	Close monitoring connections by sending the service a connection termination message with the specified bit set. Default value: FIN Possible values = RESET, FIN
vserverspecificmac	<String>	Read-write	Allow a MAC-mode virtual server to accept traffic returned by an intermediary device, such as a firewall, to which the traffic was previously forwarded by another MAC-mode virtual server.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			The second virtual server can then distribute that traffic across the destination server farm. Also useful when load balancing Branch Repeater appliances. Note: The second virtual server can also send the traffic to another set of intermediary devices, such as another set of firewalls. If necessary, you can configure multiple MAC-mode virtual servers to pass traffic successively through multiple sets of intermediary devices. Default value: DISABLED Possible values = ENABLED, DISABLED
allowboundsvcremoval	<String>	Read-write	This is used, to enable/disable the option of svc/svcgroup removal, if it is bound to one or more vserver. If it is

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			enabled, the svc/svcgroup can be removed, even if it bound to vservers. If disabled, an error will be thrown, when the user tries to remove a svc/svcgroup without unbinding from its vservers. Default value: ENABLED Possible values = ENABLED, DISABLED
retainservicestate	<String>	Read-write	This option is used to retain the original state of service or servicegroup member when an enable server command is issued. Default value: OFF Possible values = ON, OFF
dbsttl	<Integer>	Read-write	Specify the TTL for DNS record for domain based service. The default value of ttl is 0 which indicates to use the TTL received in DNS response for monitors. Default value: 0

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
maxpipelinenat	<Integer>	Read-write	Maximum number of concurrent requests to allow on a single client connection, which is identified by the <clientip:port>-<vserver ip:port> tuple. This parameter is applicable to ANY service type and all UDP service types (except DNS) and only when "svrTimeout" is set to zero. A value of 0 (zero) applies no limit to the number of concurrent requests allowed on a single client connection.
literaladccookieattribute	<String>	Read-write	String configured as LiteralADCCookieAttribute will be appended as attribute for Citrix ADC cookie (for example: LB cookie persistence , GSLB site persistence, CS cookie persistence, LB group cookie persistence). Sample usage - set lb parameter -LiteralADCCookieAttribute ";SameSite=None".

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
computedadccookieattribute	<String>	Read-write	ComputedADCCookieAttribute accepts ns variable as input in form of string starting with $ (to understand how to configure ns variable, please check man add ns variable). policies can be configured to modify this variable for every transaction and the final value of the variable after policy evaluation will be appended as attribute to Citrix ADC cookie (for example: LB cookie persistence , GSLB sitepersistence, CS cookie persistence, LB group cookie persistence). Only one of ComputedADCCookieAttribute, LiteralADCCookieAttribute can be set. Sample usage - add ns variable lbvar -type TEXT(100) -scope Transaction add ns assignment lbassign -variable $lbvar -set "\

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			\";SameSite=Strict\ \"" add rewrite policy lbpol <valid policy expression> lbassign bind rewrite global lbpol 100 next -type RES_OVERRIDE set lb param -ComputedADCCookieAttribute "$lbvar" For incoming client request, if above policy evaluates TRUE, then SameSite=Strict will be appended to ADC generated cookie.
storemqttclientidandusername	<String>	Read-write	This option allows to store the MQTT clientid and username in transactional logs. Default value: NO Possible values = YES, NO
dropmqttjumbomessage	<String>	Read-write	When this option is enabled, MQTT messages of length greater than 64k will be dropped and the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			client/server connections will be reset. Default value: YES Possible values = YES, NO
lbhashalgorithm	<String>	Read-write	This option dictates the hashing algorithm used for hash based LB methods (URLHASH, DOMAINHASH, SOURCEIPHASH, DESTINATIONIPHASH, SRCIPDESTIPHASH, SRCIPSRCPORTHASH, TOKEN, USER_TOKEN, CALLIDHASH). Default value: DEFAULT Possible values = DEFAULT, PRAC, JARH
lbhashfingers	<Integer>	Read-write	This option is used to specify the number of fingers to be used in PRAC and JARH algorithms for hash based LB methods. Increasing the number of fingers might give better distribution of traffic

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			at the expense of additional memory. Default value: 256 Minimum value = 1 Maximum value = 1024
undefaction	<String>	Read-write	Action to perform when policy evaluation creates an UNDEF condition. Available settings function as follows: * NOLBACTION - Does not consider LB action in making LB decision. * RESET - Reset the request and notify the user, so that the user can resend the request. * DROP - Drop the request without sending a response to the user. Default value: "NOLBACTION"
proximityfromself	<String>	Read-write	Use the ADC location instead of client IP for static proximity LB or GSLB decision.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: NO Possible values = YES, NO
radiusmessageauthenticator	<String>	Read-write	If enabled, NetScaler will verify the message authenticator and also generate message authenticator if not present. Default value: NO Possible values = YES, NO
sessionsthreshold	<Integer>	Read-only	This option is used to get the upper-limit on the number of persistent sessions set by the administrator for this system. Minimum value = 1
builtin	<String[]>	Read-only	. Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL
feature	<String>	Read-only	The feature to be checked while applying this config.
adccookieattributewarningmsg	<String>	Read-only	Used to describe any configuration issue with respect to ns

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			variable configured as part of set lb parameter.
lbhashalgowinsize	<Integer>	Read-only	This options allows to increase window size used in LB hashing algorithm(DEFAULT) . Default value: 16
overridepersistencyfororder	<String>	Read-only	This option is used to override persistency when order is configured for services or servicegroups. Default value: NO Possible values = YES, NO
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- UPDATE
- UNSET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbparameter **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"lbparameter":{

"httponlycookieflag":<String_value>,

"usesecuredpersistencecookie":<String_value>,

"useencryptedpersistencecookie":<String_value>,

"cookiepassphrase":<String_value>,

"consolidatedlconn":<String_value>,

"useportforhashlb":<String_value>,
```

```
"preferdirectroute":<String_value>,

"startuprrfactor":<Integer_value>,

"monitorskipmaxclient":<String_value>,

"monitorconnectionclose":<String_value>,

"vserverspecificmac":<String_value>,

"allowboundsvcremoval":<String_value>,

"retainservicestate":<String_value>,

"dbsttl":<Integer_value>,

"maxpipelinenat":<Integer_value>,

"literaladccookieattribute":<String_value>,

"computedadccookieattribute":<String_value>,

"storemqttclientidandusername":<String_value>,

"dropmqttjumbomessage":<String_value>,

"lbhashalgorithm":<String_value>,

"lbhashfingers":<Integer_value>,

"undefaction":<String_value>,

"proximityfromself":<String_value>,

"radiusmessageauthenticator":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbparameter? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"lbparameter":{

"httponlycookieflag":true,

"usesecuredpersistencecookie":true,

"useencryptedpersistencecookie":true,

"cookiepassphrase":true,

"consolidatedlconn":true,

"useportforhashlb":true,

"preferdirectroute":true,

"startuprrfactor":true,

"monitorskipmaxclient":true,

"monitorconnectionclose":true,

"vserverspecificmac":true,

"allowboundsvcremoval":true,

"retainservicestate":true,
```

```
"dbsttl":true,

"maxpipelinenat":true,

"literaladccookieattribute":true,

"computedadccookieattribute":true,

"storemqttclientidandusername":true,

"dropmqttjumbomessage":true,

"lbhashalgorithm":true,

"lbhashfingers":true,

"undefaction":true,

"proximityfromself":true,

"radiusmessageauthenticator":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbparameter **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "lbparameter": [ {

"httponlycookieflag":<String_value>,

"usesecuredpersistencecookie":<String_value>,

"useencryptedpersistencecookie":<String_value>,

"cookiepassphrase":<String_value>,

"consolidatedlconn":<String_value>,

"useportforhashlb":<String_value>,

"preferdirectroute":<String_value>,

"startuprrfactor":<Integer_value>,

"monitorskipmaxclient":<String_value>,

"monitorconnectionclose":<String_value>,

"vserverspecificmac":<String_value>,

"sessionsthreshold":<Integer_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"allowboundsvcremoval":<String_value>,

"retainservicestate":<String_value>,

"dbsttl":<Integer_value>,

"maxpipelinenat":<Integer_value>,
```

```
"literaladccookieattribute":<String_value>,

"computedadccookieattribute":<String_value>,

"adccookieattributewarningmsg":<String_value>,

"storemqttclientidandusername":<String_value>,

"dropmqttjumbomessage":<String_value>,

"lbhashalgowinsize":<Integer_value>,

"lbhashalgorithm":<String_value>,

"lbhashfingers":<Integer_value>,

"undefaction":<String_value>,

"overridepersistencyfororder":<String_value>,

"proximityfromself":<String_value>,

"radiusmessageauthenticator":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

lbpersistentsessions

Configuration for persistence session resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
vserver	<String>	Read-write	The name of the virtual server.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
nodeid	<Integer>	Read-write	Unique number that identifies the cluster node. Minimum value = 0 Maximum value = 31
persistenceparameter	<String>	Read-write	The persistence parameter whose persistence sessions are to be flushed.
type	<Integer>	Read-only	Type of Persistence.
typestring	<String>	Read-only	Type of Persistence as String.
srcip	<String>	Read-only	SOURCE IP.
srcipv6	<String>	Read-only	SOURCE IPv6 ADDRESS.
destip	<String>	Read-only	DESTINATION IP.
destipv6	<String>	Read-only	DESTINATION IPv6 ADDRESS.
flags	<Boolean>	Read-only	IPv6 FLAGS.
destport	<Integer>	Read-only	Destination port. Range 1 - 65535 * in CLI is represented as 65535 in NITRO API
vservername	<String>	Read-only	Virtual server name.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
timeout	<Integer>	Read-only	Persistent Session timeout.
referencecount	<Integer>	Read-only	Reference Count.
persistenceparam	<String>	Read-only	Specific persistence information . Callid in case of SIP_CALLID persistence entry , RTSP session id in case of RTSP_SESSIONID persistence entry.
cnamepersparam	<String>	Read-only	The cname that is selected incase of gslb service.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET (ALL)
- COUNT
- CLEAR

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

CLEAR

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbpersistentsessions? **action=clear HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"lbpersistentsessions":{

"vserver":<String_value>,

"persistenceparameter":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbpersistentsessions **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/lbpersistentsessions? **args=vserver: <String_value> ,nodeid: <Integer_value>**

Use this query-parameter to get lbpersistentsessions resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/config/lbpersistentsessions? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/lbpersistentsessions? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of lbpersistentsessions resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/lbpersistentsessions? **view=summary**

Use this query-parameter to get the summary output of lbpersistentsessions resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/lbpersistentsessions? **pagesize=#no;pageno=#no**

Use this query-parameter to get the lbpersistentsessions resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "lbpersistentsessions": [ {

vserver:<String_value>,nodeid:<Integer_value>"type":<Integer_value>,

"typestring":<String_value>,

"srcip":<String_value>,

"srcipv6":<String_value>,

"destip":<String_value>,

"destipv6":<String_value>,

"flags":<Boolean_value>,

"destport":<Integer_value>,

"vservername":<String_value>,

"timeout":<Integer_value>,

"referencecount":<Integer_value>,

"sipcallid":<String_value>,

"persistenceparam":<String_value>,

"cnamepersparam":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbpersistentsessions? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "lbpersistentsessions": [ { "__count": "#no"} ] }
```

lbpolicy

Configuration for lb policy resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the LB policy. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			characters. Can be changed after the LB policy is added. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my lb policy" or 'my lb policy').
rule	<String>	Read-write	Expression against which traffic is evaluated.
action	<String>	Read-write	Name of action to use if the request matches this LB policy.
undefaction	<String>	Read-write	Action to perform if the result of policy evaluation is undefined (UNDEF). An UNDEF event indicates an internal error condition. Available settings function as follows: * NOLBACTION - Does not consider

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			LB actions in making LB decision. * RESET - Reset the request and notify the user, so that the user can resend the request. * DROP - Drop the request without sending a response to the user.
logaction	<String>	Read-write	Name of the messagelog action to use for requests that match this policy.
comment	<String>	Read-write	Any type of information about this LB policy.
newname	<String>	Read-write	New name for the LB policy. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space ( ), at (@), equals (=), colon (:), and underscore characters. The following requirement applies

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my lb policy" or 'my lb policy'). Minimum length = 1
hits	<Integer>	Read-only	Number of hits.
undefhits	<Integer>	Read-only	Number of policy UNDEF hits.
feature	<String>	Read-only	The feature to be checked while applying this config.
builtin	<String[]>	Read-only	Flag to determine if LB policy is built-in or not. Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT
- RENAME

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbpolicy **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"lbpolicy":{

<b>"name":<String_value>,

</b><b>"rule":<String_value>,

</b><b>"action":<String_value>,

</b>"undefaction":<String_value>,

"logaction":<String_value>,

"comment":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbpolicy/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbpolicy **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"lbpolicy":{

<b>"name":<String_value>,

</b>"rule":<String_value>,

"action":<String_value>,

"undefaction":<String_value>,

"logaction":<String_value>,

"comment":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbpolicy? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"lbpolicy":{

<b>"name":<String_value>,

</b>"undefaction":true,

"logaction":true,

"comment":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

RENAME

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbpolicy? **action=rename HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"lbpolicy":{

<b>"name":<String_value>,

</b><b>"newname":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbpolicy **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/lbpolicy? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/lbpolicy? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of lbpolicy resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/lbpolicy? **view=summary**

Use this query-parameter to get the summary output of lbpolicy resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/lbpolicy? **pagesize=#no;pageno=#no**

Use this query-parameter to get the lbpolicy resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "lbpolicy": [ {

"name":<String_value>,

"rule":<String_value>,

"action":<String_value>,

"undefaction":<String_value>,

"hits":<Integer_value>,

"undefhits":<Integer_value>,

"comment":<String_value>,

"feature":<String_value>,

"builtin":<String[]_value>,

"logaction":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbpolicy/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/lbpolicy/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/lbpolicy/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of lbpolicy resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lbpolicy": [ {

"name":<String_value>,

"rule":<String_value>,

"action":<String_value>,

"undefaction":<String_value>,

"hits":<Integer_value>,

"undefhits":<Integer_value>,

"comment":<String_value>,

"feature":<String_value>,

"builtin":<String[]_value>,

"logaction":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbpolicy? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "lbpolicy": [ { "__count": "#no"} ] }
```

lbpolicy_binding

Binding object which returns the resources bound to lbpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the LB policy. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#),

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			space ( ), at (@), equals (=), colon (:), and underscore characters. Can be changed after the LB policy is added. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my lb policy" or 'my lb policy').
lbpolicy_lbpolicylabel_binding	<lbpolicy_lbpolicylabel_binding[]>	Read-only	lbpolicylabel that can be bound to lbpolicy.
lbpolicy_lbglobal_binding	<lbpolicy_lbglobal_binding[]>	Read-only	lbglobal that can be bound to lbpolicy.
lbpolicy_lbvserver_binding	<lbpolicy_lbvserver_binding[]>	Read-only	lbvserver that can be bound to lbpolicy.
lbpolicy_gslbvserver_binding	<lbpolicy_gslbvserver_binding[]>	Read-only	gslbvserver that can be bound to lbpolicy.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbpolicy_binding/ name_value<String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "lbpolicy_binding": [ {

"name":<String_value>,

"lbpolicy_gslbvserver_binding":<lbpolicy_gslbvserver_binding[]_value>,

"lbpolicy_lbpolicylabel_binding":<lbpolicy_lbpolicylabel_binding[]_value>,

"lbpolicy_lbvserver_binding":<lbpolicy_lbvserver_binding[]_value>,

"lbpolicy_lbglobal_binding":<lbpolicy_lbglobal_binding[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbpolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/lbpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "lbpolicy_binding": [ {

"name":<String_value>,

"lbpolicy_gslbvserver_binding":<lbpolicy_gslbvserver_binding[]_value>,

"lbpolicy_lbpolicylabel_binding":<lbpolicy_lbpolicylabel_binding[]_value>,

"lbpolicy_lbvserver_binding":<lbpolicy_lbvserver_binding[]_value>,

"lbpolicy_lbglobal_binding":<lbpolicy_lbglobal_binding[]_value>

}]}
```

lbpolicy_gslbvserver_binding

Binding object showing the gslbvserver that can be bound to lbpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the LB policy. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Can be changed after the LB policy is added. The following

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my lb policy" or 'my lb policy').
boundto	<String>	Read-write	Location where policy is bound.
gotopriorityexpression	<String>	Read-only	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
priority	<Integer>	Read-only	Specifies the priority of the policy.
activepolicy	<Integer>	Read-only	Indicates whether policy is bound or not.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbpolicy_gslbvserver_binding/ name_value<String>

Query-parameters:

filter

http:// <netscaler-ip-address> /nitro/v1/config/lbpolicy_gslbvserver_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of lbpolicy_gslbvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination

http:// <netscaler-ip-address> /nitro/v1/config/lbpolicy_gslbvserver_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the lbpolicy_gslbvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lbpolicy_gslbvserver_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"gotopriorityexpression":<String_value>,

"priority":<Integer_value>,

"activepolicy":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbpolicy_gslbvserver_binding

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters:

bulkbindings

http:// <netscaler-ip-address> /nitro/v1/config/lbpolicy_gslbvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lbpolicy_gslbvserver_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"gotopriorityexpression":<String_value>,

"priority":<Integer_value>,

"activepolicy":<Integer_value>

}]}
```

```
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbpolicy_gslbvserver_binding/ name_value<String> ? **count=yes**

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"lbpolicy_gslbvserver_binding": [ { "__count": "#no"} ] }
```

lbpolicy_lbglobal_binding

Binding object showing the lbglobal that can be bound to lbpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the LB policy. Must begin

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Can be changed after the LB policy is added. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my lb policy" or 'my lb policy').
boundto	<String>	Read-write	Location where policy is bound.
labelname	<String>	Read-only	Name of the label to invoke if the current policy rule evaluates to TRUE.
gotopriorityexpression	<String>	Read-only	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
activepolicy	<Integer>	Read-only	Indicates whether policy is bound or not.
labeltype	<String>	Read-only	Type of policy label invocation. Possible values = reqvserver, policylabel
priority	<Integer>	Read-only	Specifies the priority of the policy.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbpolicy_lbglobal_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/lbpolicy_lbglobal_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of lbpolicy_lbglobal_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/lbpolicy_lbglobal_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the lbpolicy_lbglobal_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lbpolicy_lbglobal_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"labelname":<String_value>,

"gotopriorityexpression":<String_value>,

"activepolicy":<Integer_value>,

"labeltype":<String_value>,

"priority":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbpolicy_lbglobal_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/lbpolicy_lbglobal_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lbpolicy_lbglobal_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"labelname":<String_value>,

"gotopriorityexpression":<String_value>,

"activepolicy":<Integer_value>,

"labeltype":<String_value>,

"priority":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbpolicy_lbglobal_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"lbpolicy_lbglobal_binding": [ { "__count": "#no"} ] }
```

lbpolicy_lbpolicylabel_binding

Binding object showing the lbpolicylabel that can be bound to lbpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
boundto	<String>	Read-write	Location where policy is bound.
name	<String>	Read-write	Name of the LB policy. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Can be changed after the LB policy is added. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my lb policy" or 'my lb policy').

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
priority	<Integer>	Read-only	Specifies the priority of the policy.
labeltype	<String>	Read-only	Type of policy label invocation. Possible values = reqvserver, policylabel
activepolicy	<Integer>	Read-only	Indicates whether policy is bound or not.
gotopriorityexpression	<String>	Read-only	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
labelname	<String>	Read-only	Name of the label to invoke if the current policy rule evaluates to TRUE.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbpolicy_lbpolicylabel_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ lbpolicy_lbpolicylabel_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of lbpolicy_lbpolicylabel_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/lbpolicy_lbpolicylabel_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the lbpolicy_lbpolicylabel_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lbpolicy_lbpolicylabel_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"priority":<Integer_value>,

"labeltype":<String_value>,

"activepolicy":<Integer_value>,

"gotopriorityexpression":<String_value>,

"labelname":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbpolicy_lbpolicylabel_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/lbpolicy_lbpolicylabel_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lbpolicy_lbpolicylabel_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"priority":<Integer_value>,

"labeltype":<String_value>,

"activepolicy":<Integer_value>,

"gotopriorityexpression":<String_value>,

"labelname":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbpolicy_lbpolicylabel_binding/name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"lbpolicy_lbpolicylabel_binding": [ { "__count": "#no"} ] }
```

lbpolicy_lbvserver_binding

Binding object showing the lbvserver that can be bound to lbpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the LB policy. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Can be changed after the LB policy is added. The following

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my lb policy" or 'my lb policy').
boundto	<String>	Read-write	Location where policy is bound.
labeltype	<String>	Read-only	Type of policy label invocation. Possible values = reqvserver, policylabel
priority	<Integer>	Read-only	Specifies the priority of the policy.
labelname	<String>	Read-only	Name of the label to invoke if the current policy rule evaluates to TRUE.
gotopriorityexpression	<String>	Read-only	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
activepolicy	<Integer>	Read-only	Indicates whether policy is bound or not.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbpolicy_lbvserver_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ lbpolicy_lbvserver_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of lbpolicy_lbvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/lbpolicy_lbvserver_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the lbpolicy_lbvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lbpolicy_lbvserver_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"labelname":<String_value>,
```

```
"gotopriorityexpression":<String_value>,

"activepolicy":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbpolicy_lbvserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/lbpolicy_lbvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lbpolicy_lbvserver_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,
```

```
"labelname":<String_value>,

"gotopriorityexpression":<String_value>,

"activepolicy":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbpolicy_lbvserver_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"lbpolicy_lbvserver_binding": [ { "__count": "#no"} ] }
```

lbpolicylabel

Configuration for lb policy label resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
labelname	<String>	Read-write	Name for the LB policy label. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space ( ), at (@), equals (=), colon (:), and underscore characters. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my lb policy label" or 'my lb policy label').
policylabeltype	<String>	Read-write	Protocols supported by the policylabel. Available Types are : * HTTP - HTTP requests. * DNS - DNS request.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			* OTHERTCP - OTHERTCP request. * SIP_UDP - SIP_UDP request. * SIP_TCP - SIP_TCP request. * MYSQL - MYSQL request. * MSSQL - MSSQL request. * ORACLE - ORACLE request. * NAT - NAT request. * DIAMETER - DIAMETER request. * RADIUS - RADIUS request. * MQTT - MQTT request. * QUIC_BRIDGE - QUIC_BRIDGE request. * HTTP_QUIC - HTTP_QUIC request.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: HTTP Possible values = HTTP, OTHERTCP, SIP_UDP, SIP_TCP, MYSQL, MSSQL, ORACLE, NAT, DIAMETER, RADIUS, DNS, MQTT, QUIC_BRIDGE, HTTP_QUIC
comment	<String>	Read-write	Any comments to preserve information about this LB policy label.
newname	<String>	Read-write	New name for the LB policy label. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Minimum length = 1
numpol	<Integer>	Read-only	number of polices bound to label.
hits	<Integer>	Read-only	Number of times policy label was invoked.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
gotopriorityexpression	<String>	Read-only	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
labeltype	<String>	Read-only	Type of policy label to invoke. Available settings function as follows: * vserver - Invokes the unnamed policy label associated with the specified virtual server. * policylabel - Invoke a user-defined policy label. Possible values = reqvserver, policylabel
invoke_labelname	<String>	Read-only	* If labelType is policylabel, name of the policy label to invoke. * If labelType is reqvserver, name of the virtual server.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET (ALL)
- GET
- COUNT
- RENAME

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbpolicylabel **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"lbpolicylabel":{

<b>"labelname":<String_value>,

</b>"policylabeltype":<String_value>,

"comment":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbpolicylabel/ labelname_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

RENAME

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbpolicylabel? **action=rename HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"lbpolicylabel":{

<b>"labelname":<String_value>,

</b><b>"newname":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbpolicylabel **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/lbpolicylabel? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/lbpolicylabel? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of lbpolicylabel resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/lbpolicylabel? **view=summary**

Use this query-parameter to get the summary output of lbpolicylabel resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/lbpolicylabel? **pagesize=#no;pageno=#no**

Use this query-parameter to get the lbpolicylabel resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "lbpolicylabel": [ {

"labelname":<String_value>,

"policylabeltype":<String_value>,

"numpol":<Integer_value>,

"hits":<Integer_value>,

"comment":<String_value>,

"gotopriorityexpression":<String_value>,

"labeltype":<String_value>,

"invoke_labelname":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbpolicylabel/ labelname_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/lbpolicylabel/ labelname_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/lbpolicylabel/ labelname_value<String> ? **view=summary**

Use this query-parameter to get the summary output of lbpolicylabel resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lbpolicylabel": [ {

"labelname":<String_value>,

"policylabeltype":<String_value>,

"numpol":<Integer_value>,

"hits":<Integer_value>,
```

```
"comment":<String_value>,

"gotopriorityexpression":<String_value>,

"labeltype":<String_value>,

"invoke_labelname":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbpolicylabel? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "lbpolicylabel": [ { "__count": "#no"} ] }
```

lbpolicylabel_binding

Binding object which returns the resources bound to lbpolicylabel.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
labelname	<String>	Read-write	Name for the LB policy label. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space ( ), at (@), equals (=), colon (:), and underscore characters. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my lb policy label" or 'my lb policy label').
lbpolicylabel_policybinding_binding	<lbpolicylabel_policybinding_binding[]>	Read-only	policybinding that can be bound to lbpolicylabel.
lbpolicylabel_lbpolicy_binding	<lbpolicylabel_lbpolicy_binding[]>	Read-only	lbpolicy that can be bound to lbpolicylabel.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbpolicylabel_binding/ labelname_value<String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "lbpolicylabel_binding": [ {

"labelname":<String_value>,

"lbpolicylabel_lbpolicy_binding":<lbpolicylabel_lbpolicy_binding[]_value>,

"lbpolicylabel_policybinding_binding":<lbpolicylabel_policybinding_binding
[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbpolicylabel_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/lbpolicylabel_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "lbpolicylabel_binding": [ {

"labelname":<String_value>,

"lbpolicylabel_lbpolicy_binding":<lbpolicylabel_lbpolicy_binding[]_value>,

"lbpolicylabel_policybinding_binding":<lbpolicylabel_policybinding_binding
[]_value>

}]}
```

lbpolicylabel_lbpolicy_binding

Binding object showing the lbpolicy that can be bound to lbpolicylabel.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
labelname	<String>	Read-write	Name for the LB policy label. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space ( ), at (@), equals (=), colon (:), and underscore characters.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my lb policy label" or 'my lb policy label').

Possible values = reqvserver, policylabel

```
 </td></tr><tr><td>invoke

 </td><td>&lt;Boolean&gt;

 </td><td>Read-write

 </td><td>If the current policy evaluates to TRUE, terminate evaluation of
policies bound to the current policy label and evaluate the specified
policy label.

 </td></tr><tr><td>gotopriorityexpression

 </td><td>&lt;String&gt;

 </td><td>Read-write

 </td><td>Expression specifying the priority of the next policy which will
get evaluated if the current policy rule evaluates to TRUE.

 </td></tr><tr><td>policyname

 </td><td>&lt;String&gt;

 </td><td>Read-write

 </td><td>Name of the LB policy.

 </td></tr><tr><td>invoke_labelname

 </td><td>&lt;String&gt;

 </td><td>Read-write

 </td><td>* If labelType is policylabel, name of the policy label to
invoke.
```

- If labelType is reqvserver, name of the virtual server.

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/lbpolicylabel_lbpolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"lbpolicylabel_lbpolicy_binding":{

<b>"labelname":<String_value>,

</b><b>"policyname":<String_value>,

</b><b>"priority":<Integer_value>,

</b>"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>,

"labeltype":<String_value>,

"invoke_labelname":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbpolicylabel_lbpolicy_binding/ labelname_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ lbpolicylabel_lbpolicy_binding/ labelname_value<String> ? **args= policyname:<String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbpolicylabel_lbpolicy_binding/ labelname_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ lbpolicylabel_lbpolicy_binding/ labelname_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of lbpolicylabel_lbpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/lbpolicylabel_lbpolicy_binding/ labelname_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the lbpolicylabel_lbpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lbpolicylabel_lbpolicy_binding": [ {

"labelname":<String_value>,

"priority":<Integer_value>,
```

```
"labeltype":<String_value>,

"invoke":<Boolean_value>,

"gotopriorityexpression":<String_value>,

"policyname":<String_value>,

"invoke_labelname":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbpolicylabel_lbpolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/lbpolicylabel_lbpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lbpolicylabel_lbpolicy_binding": [ {

"labelname":<String_value>,

"priority":<Integer_value>,

"labeltype":<String_value>,

"invoke":<Boolean_value>,

"gotopriorityexpression":<String_value>,

"policyname":<String_value>,

"invoke_labelname":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbpolicylabel_lbpolicy_binding/ labelname_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"lbpolicylabel_lbpolicy_binding": [ { "__count": "#no"} ] }
```

lbpolicylabel_policybinding_binding

Binding object showing the policybinding that can be bound to lbpolicylabel.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
priority	<Integer>	Read-write	Specifies the priority of the policy.
labeltype	<String>	Read-write	Type of policy label to invoke. Available settings function as follows: * vserver - Invokes the unnamed policy label associated with the specified virtual server. * policylabel - Invoke a user-defined policy label. Possible values = reqvserver, policylabel
labelname	<String>	Read-write	Name for the LB policy label. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space ( ), at (@), equals (=), colon (:), and underscore characters.

The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my lb policy label" or 'my lb policy label').

```
</td></tr><tr><td>__count

</td><td>&lt;Double&gt;

</td><td>Read-write

</td><td>count parameter

</td></tr></tbody></table>
```

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbpolicylabel_policybinding_binding/ labelname_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ lbpolicylabel_policybinding_binding/ labelname_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of lbpolicylabel_policybinding_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/lbpolicylabel_policybinding_binding/ labelname_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the lbpolicylabel_policybinding_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lbpolicylabel_policybinding_binding": [ {

"priority":<Integer_value>,
```

```
"labeltype":<String_value>,

"labelname":<String_value>,

"invoke":<Boolean_value>,

"gotopriorityexpression":<String_value>,

"policyname":<String_value>,

"invoke_labelname":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbpolicylabel_policybinding_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/lbpolicylabel_policybinding_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lbpolicylabel_policybinding_binding": [ {

"priority":<Integer_value>,

"labeltype":<String_value>,

"labelname":<String_value>,

"invoke":<Boolean_value>,

"gotopriorityexpression":<String_value>,

"policyname":<String_value>,

"invoke_labelname":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbpolicylabel_policybinding_binding/ labelname_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"lbpolicylabel_policybinding_binding": [ { "__count": "#no"} ] }
```

lbprofile

Configuration for LB profile resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
lbprofilename	<String>	Read-write	Name of the LB profile. Minimum length = 1
dbslb	<String>	Read-write	Enable database specific load balancing for MySQL and MSSQL service types. Default value: DISABLED Possible values = ENABLED, DISABLED
processlocal	<String>	Read-write	By turning on this option packets destined to a vserver in a cluster will not under go any steering. Turn this option for single pa cket request response mode or when the upstream device is performing a proper RSS for connection based distribution.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: DISABLED Possible values = ENABLED, DISABLED
httponlycookieflag	<String>	Read-write	Include the HttpOnly attribute in persistence cookies. The HttpOnly attribute limits the scope of a cookie to HTTP requests and helps mitigate the risk of cross-site scripting attacks. Default value: ENABLED Possible values = ENABLED, DISABLED
cookiepassphrase	<String>	Read-write	Use this parameter to specify the passphrase used to generate secured persistence cookie value. It specifies the passphrase with a maximum of 31 characters.
usesecuredpersistencecookie	<String>	Read-write	Encode persistence cookie values using SHA2 hash. Default value: DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ENABLED, DISABLED
useencryptedpersistencecookie	<String>	Read-write	Encode persistence cookie values using SHA2 hash. Default value: DISABLED Possible values = ENABLED, DISABLED
literaladccookieattribute	<String>	Read-write	String configured as LiteralADCCookieAttribute will be appended as attribute for Citrix ADC cookie (for example: LB cookie persistence , GSLB site persistence, CS cookie persistence, LB group cookie persistence). Sample usage - add lb profile lbprof -LiteralADCCookieAttribute ";SameSite=None".
computedadccookieattribute	<String>	Read-write	ComputedADCCookieAttribute accepts ns variable as input in form of string starting with $ (to understand how to configure ns variable, please

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			check man add ns variable). policies can be configured to modify this variable for every transaction and the final value of the variable after policy evaluation will be appended as attribute to Citrix ADC cookie (for example: LB cookie persistence , GSLB sitepersistence, CS cookie persistence, LB group cookie persistence). Only one of ComputedADCCookieAttribute, LiteralADCCookieAttribute can be set. Sample usage - add ns variable lbvar -type TEXT(100) -scope Transaction add ns assignment lbassign -variable $lbvar -set "\\";SameSite=Strict\\"" add rewrite policy lbpol <valid policy expression> lbassign

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			bind rewrite global lbpol 100 next -type RES_OVERRIDE add lb profile lbprof -ComputedADCCookieAttribute "$lbvar" For incoming client request, if above policy evaluates TRUE, then SameSite=Strict will be appended to ADC generated cookie.
storemqttclientidandusername	<String>	Read-write	This option allows to store the MQTT clientid and username in transactional logs. Default value: NO Possible values = YES, NO
lbhashalgorithm	<String>	Read-write	This option dictates the hashing algorithm used for hash based LB methods (URLHASH, DOMAINHASH, SOURCEIPHASH, DESTINATIONIPHASH, SRCIPDESTIPHASH, SRCIPSRCPORTHA

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			SH, TOKEN, USER_TOKEN, CALLIDHASH). Default value: DEFAULT Possible values = DEFAULT, PRAC, JARH
lbhashfingers	<Integer>	Read-write	This option is used to specify the number of fingers to be used in PRAC and JARH algorithms for hash based LB methods. Increasing the number of fingers might give better distribution of traffic at the expense of additional memory. Default value: 256 Minimum value = 1 Maximum value = 1024
proximityfromself	<String>	Read-write	Use the ADC location instead of client IP for static proximity LB or GSLB decision. Default value: NO Possible values = YES, NO

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
vsvrcount	<Integer>	Read-only	Total number of vservers , the profile is bound to.
adccookieattributewarningmsg	<String>	Read-only	Used to describe any configuration issue with respect to ns variable configured as part of add/set lb profile.
lbhashalgowinsize	<Integer>	Read-only	This options allows to increase window size used in LB hashing algorithm(DEFAULT) . Default value: 16
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbprofile **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"lbprofile":{

<b>"lbprofilename":<String_value>,

</b>"dbslb":<String_value>,

"processlocal":<String_value>,
```

```
"httponlycookieflag":<String_value>,

"cookiepassphrase":<String_value>,

"usesecuredpersistencecookie":<String_value>,

"useencryptedpersistencecookie":<String_value>,

"literaladccookieattribute":<String_value>,

"computedadccookieattribute":<String_value>,

"storemqttclientidandusername":<String_value>,

"lbhashalgorithm":<String_value>,

"lbhashfingers":<Integer_value>,

"proximityfromself":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbprofile/ lbprofilename_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbprofile **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"lbprofile":{

<b>"lbprofilename":<String_value>,

</b>"dbslb":<String_value>,

"processlocal":<String_value>,

"httponlycookieflag":<String_value>,

"cookiepassphrase":<String_value>,

"usesecuredpersistencecookie":<String_value>,

"useencryptedpersistencecookie":<String_value>,

"literaladccookieattribute":<String_value>,

"computedadccookieattribute":<String_value>,

"storemqttclientidandusername":<String_value>,

"lbhashalgorithm":<String_value>,

"lbhashfingers":<Integer_value>,

"proximityfromself":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbprofile? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"lbprofile":{

<b>"lbprofilename":<String_value>,

</b>"dbslb":true,

"processlocal":true,

"httponlycookieflag":true,

"cookiepassphrase":true,

"usesecuredpersistencecookie":true,

"useencryptedpersistencecookie":true,

"literaladccookieattribute":true,

"computedadccookieattribute":true,

"storemqttclientidandusername":true,

"lbhashalgorithm":true,

"lbhashfingers":true,

"proximityfromself":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbprofile **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/lbprofile? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/lbprofile? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of lbprofile resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/lbprofile? **view=summary**

Use this query-parameter to get the summary output of lbprofile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/lbprofile? **pagesize=#no;pageno=#no**

Use this query-parameter to get the lbprofile resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "lbprofile": [ {

"lbprofilename":<String_value>,

"dbslb":<String_value>,

"processlocal":<String_value>,

"httponlycookieflag":<String_value>,

"cookiepassphrase":<String_value>,

"usesecuredpersistencecookie":<String_value>,

"useencryptedpersistencecookie":<String_value>,

"vsvrcount":<Integer_value>,

"literaladccookieattribute":<String_value>,

"computedadccookieattribute":<String_value>,

"adccookieattributewarningmsg":<String_value>,

"storemqttclientidandusername":<String_value>,

"lbhashalgowinsize":<Integer_value>,

"lbhashalgorithm":<String_value>,

"lbhashfingers":<Integer_value>,

"proximityfromself":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbprofile/ lbprofilename_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/lbprofile/ lbprofilename_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/lbprofile/ lbprofilename_value<String> ? **view=summary**

Use this query-parameter to get the summary output of lbprofile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lbprofile": [ {

"lbprofilename":<String_value>,

"dbslb":<String_value>,

"processlocal":<String_value>,

"httponlycookieflag":<String_value>,
```

```
"cookiepassphrase":<String_value>,

"usesecuredpersistencecookie":<String_value>,

"useencryptedpersistencecookie":<String_value>,

"vsvrcount":<Integer_value>,

"literaladccookieattribute":<String_value>,

"computedadccookieattribute":<String_value>,

"adccookieattributewarningmsg":<String_value>,

"storemqttclientidandusername":<String_value>,

"lbhashalgowinsize":<Integer_value>,

"lbhashalgorithm":<String_value>,

"lbhashfingers":<Integer_value>,

"proximityfromself":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbprofile? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "lbprofile": [ { "__count": "#no"} ] }
```

lbroute

Configuration for LB route resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
network	<String>	Read-write	The IP address of the network to which the route belongs.
netmask	<String>	Read-write	The netmask to which the route belongs.
gatewayname	<String>	Read-write	The name of the route. Minimum length = 1
td	<Integer>	Read-write	Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0. Default value: 0

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum value = 0 Maximum value = 4094
flags	<String>	Read-only	State of the configured gateway. Possible values = UP, DOWN, UNKNOWN, BUSY, OUT OF SERVICE, GOING OUT OF SERVICE, DOWN WHEN GOING OUT OF SERVICE, NS_EMPTY_STR, Unknown, DISABLED
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbroute **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"lbroute":{

<b>"network":<String_value>,

</b><b>"netmask":<String_value>,

</b><b>"gatewayname":<String_value>,

</b>"td":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbroute/ network_value<String> **Query-parameters: args= netmask:<String_value>, td: <Integer_value>**
get (all)
URL: http:// <netscaler-ip-address> /nitro/v1/config/lbroute **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/lbroute? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/lbroute? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of lbroute resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/lbroute? **view=summary**

Use this query-parameter to get the summary output of lbroute resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/lbroute? **pagesize=#no;pageno=#no**

Use this query-parameter to get the lbroute resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "lbroute": [ {

"network":<String_value>,

"netmask":<String_value>,

"td":<Integer_value>,

"gatewayname":<String_value>,

"flags":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

count
URL: http:// <netscaler-ip-address> /nitro/v1/config/lbroute? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "lbroute": [ { "__count": "#no"} ] }
```

lbroute6

Configuration for LB route6 resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
network	<String>	Read-write	The destination network.
gatewayname	<String>	Read-write	The name of the route. Minimum length = 1
td	<Integer>	Read-write	Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0. Default value: 0 Minimum value = 0 Maximum value = 4094
flags	<String>	Read-only	State of the configured gateway. Possible values = UP, DOWN, UNKNOWN, BUSY,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			OUT OF SERVICE, GOING OUT OF SERVICE, DOWN WHEN GOING OUT OF SERVICE, NS_EMPTY_STR, Unknown, DISABLED
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbroute6 **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"lbroute6":{

<b>"network":<String_value>,

</b><b>"gatewayname":<String_value>,

</b>"td":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbroute6/ network_value<String> **Query-parameters: args=td: <Integer_value>**
get (all)
URL: http:// <netscaler-ip-address> /nitro/v1/config/lbroute6 **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/lbroute6? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/lbroute6? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of lbroute6 resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/lbroute6? **view=summary**

Use this query-parameter to get the summary output of lbroute6 resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/lbroute6? **pagesize=#no;pageno=#no**

Use this query-parameter to get the lbroute6 resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "lbroute6": [ {

"network":<String_value>,

"td":<Integer_value>,

"gatewayname":<String_value>,
```

```
"flags":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

count

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbroute6? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "lbroute6": [ { "__count": "#no"} ] }
```

lbsipparameters

Configuration for SIP parameters resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
rnatsrcport	<Integer>	Read-write	Port number with which to match the source port in server-

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			initiated SIP traffic. The rport parameter is added, without a value, to SIP packets that have a matching source port number, and CALL-ID based persistence is implemented for the responses received by the virtual server. Default value: 0
rnatdstport	<Integer>	Read-write	Port number with which to match the destination port in server-initiated SIP traffic. The rport parameter is added, without a value, to SIP packets that have a matching destination port number, and CALL-ID based persistence is implemented for the responses received by the virtual server. Default value: 0
retrydur	<Integer>	Read-write	Time, in seconds, for which a client must wait before initiating a connection after receiving a 503 Service Unavailable response from the SIP server. The time value is sent in the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			"Retry-After" header in the 503 response. Default value: 120 Minimum value = 1
addrportvip	<String>	Read-write	Add the rport parameter to the VIA headers of SIP requests that virtual servers receive from clients or servers. Default value: ENABLED Possible values = ENABLED, DISABLED
sip503ratethreshold	<Integer>	Read-write	Maximum number of 503 Service Unavailable responses to generate, once every 10 milliseconds, when a SIP virtual server becomes unavailable. Default value: 100
rnatsecuresrcport	<Integer>	Read-write	Port number with which to match the source port in server-initiated SIP over SSL traffic. The rport parameter is added, without a value, to SIP packets that have a matching source port number, and CALL-ID based

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			persistence is implemented for the responses received by the virtual server. Default value: 0 Range 1 - 65535 * in CLI is represented as 65535 in NITRO API
rnatsecuredstport	<Integer>	Read-write	Port number with which to match the destination port in server-initiated SIP over SSL traffic. The rport parameter is added, without a value, to SIP packets that have a matching destination port number, and CALL-ID based persistence is implemented for the responses received by the virtual server. Default value: 0 Range 1 - 65535 * in CLI is represented as 65535 in NITRO API

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
builtin	<String[]>	Read-only	Flag to determine if SIP param is built-in or not. Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL
feature	<String>	Read-only	The feature to be checked while applying this config.
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- UPDATE
- UNSET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.
- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbsipparameters **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"lbsipparameters":{

"rnatsrcport":<Integer_value>,

"rnatdstport":<Integer_value>,

"retrydur":<Integer_value>,

"addrportvip":<String_value>,

"sip503ratethreshold":<Integer_value>,

"rnatsecuresrcport":<Integer_value>,

"rnatsecuredstport":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbsipparameters? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"lbsipparameters":{

"rnatsrcport":true,

"rnatdstport":true,

"retrydur":true,

"addrportvip":true,

"sip503ratethreshold":true,

"rnatsecuresrcport":true,

"rnatsecuredstport":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbsipparameters **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "lbsipparameters": [ {

"rnatsrcport":<Integer_value>,

"rnatdstport":<Integer_value>,

"retrydur":<Integer_value>,

"addrportvip":<String_value>,

"sip503ratethreshold":<Integer_value>,

"rnatsecuresrcport":<Integer_value>,

"rnatsecuredstport":<Integer_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

lbvserver

Configuration for Load Balancing Virtual Server resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the virtual server. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at sign (@), equal sign (=), and hyphen (-) characters. Can be changed after the virtual server is created. CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my vserver" or 'my vserver'). . Minimum length = 1
servicetype	<String>	Read-write	Protocol used by the service (also called the service type). Possible values = HTTP, FTP, TCP, UDP, SSL, SSL_BRIDGE,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			SSL_TCP, DTLS, NNTP, DNS, DHCPRA, ANY, SIP_UDP, SIP_TCP, SIP_SSL, DNS_TCP, RTSP, PUSH, SSL_PUSH, RADIUS, RDP, MYSQL, MSSQL, DIAMETER, SSL_DIAMETER, TFTP, ORACLE, SMPP, SYSLOGTCP, SYSLOGUDP, FIX, SSL_FIX, PROXY, USER_TCP, USER_SSL_TCP, QUIC, IPFIX, LOGSTREAM, MONGO, MONGO_TLS, MQTT, MQTT_TLS, QUIC_BRIDGE, HTTP_QUIC, DOT, SSL_PROXY, KAFKA_PRODUCER
ipv46	<String>	Read-write	IPv4 or IPv6 address to assign to the virtual server.
ippattern	<String>	Read-write	IP address pattern, in dotted decimal notation, for identifying packets to

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			be accepted by the virtual server. The IP Mask parameter specifies which part of the destination IP address is matched against the pattern. Mutually exclusive with the IP Address parameter. For example, if the IP pattern assigned to the virtual server is 198.51.100.0 and the IP mask is 255.255.240.0 (a forward mask), the first 20 bits in the destination IP addresses are matched with the first 20 bits in the pattern. The virtual server accepts requests with IP addresses that range from 198.51.96.1 to 198.51.111.254. You can also use a pattern such as 0.0.2.2 and a mask such as 0.0.255.255 (a reverse mask). If a destination IP address matches

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			more than one IP pattern, the pattern with the longest match is selected, and the associated virtual server processes the request. For example, if virtual servers vs1 and vs2 have the same IP pattern, 0.0.100.128, but different IP masks of 0.0.255.255 and 0.0.224.255, a destination IP address of 198.51.100.128 has the longest match with the IP pattern of vs1. If a destination IP address matches two or more virtual servers to the same extent, the request is processed by the virtual server whose port number matches the port number in the request.
ipmask	<String>	Read-write	IP mask, in dotted decimal notation, for

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			the IP Pattern parameter. Can have leading or trailing non-zero octets (for example, 255.255.240.0 or 0.0.255.255). Accordingly, the mask specifies whether the first n bits or the last n bits of the destination IP address in a client request are to be matched with the corresponding bits in the IP pattern. The former is called a forward mask. The latter is called a reverse mask.
port	<Integer>	Read-write	Port number for the virtual server. Range 1 - 65535 * in CLI is represented as 65535 in NITRO API
ipset	<String>	Read-write	The list of IPv4/IPv6 addresses bound to ipset would form a part of listening service on the current lb vserver. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
range	<Integer>	Read-write	Number of IP addresses that the appliance must generate and assign to the virtual server. The virtual server then functions as a network virtual server, accepting traffic on any of the generated IP addresses. The IP addresses are generated automatically, as follows: * For a range of n, the last octet of the address specified by the IP Address parameter increments n-1 times. * If the last octet exceeds 255, it rolls over to 0 and the third octet increments by 1. Note: The Range parameter assigns multiple IP addresses to one virtual server. To generate an array of virtual servers, each of which owns only

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			one IP address, use brackets in the IP Address and Name parameters to specify the range. For example: add lb vserver my_vserver[1-3] HTTP 192.0.2.[1-3] 80. Default value: 1 Minimum value = 1 Maximum value = 254
persistencetype	<String>	Read-write	Type of persistence for the virtual server. Available settings function as follows: * SOURCEIP - Connections from the same client IP address belong to the same persistence session. * COOKIEINSERT - Connections that have the same HTTP Cookie, inserted by a Set-Cookie directive from a server, belong to the same

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			persistence session. * SSLSESSION - Connections that have the same SSL Session ID belong to the same persistence session. * CUSTOMSERVERID - Connections with the same server ID form part of the same session. For this persistence type, set the Server ID (CustomServerID) parameter for each service and configure the Rule parameter to identify the server ID in a request. * RULE - All connections that match a user defined rule belong to the same persistence session.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			* URLPASSIVE - Requests that have the same server ID in the URL query belong to the same persistence session. The server ID is the hexadecimal representation of the IP address and port of the service to which the request must be forwarded. This persistence type requires a rule to identify the server ID in the request. * DESTIP - Connections to the same destination IP address belong to the same persistence session. * SRCIPDESTIP - Connections that have the same source IP address and destination IP address belong to the same persistence session.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			* CALLID - Connections that have the same CALL-ID SIP header belong to the same persistence session. * RTSPSID - Connections that have the same RTSP Session ID belong to the same persistence session. * FIXSESSION - Connections that have the same SenderCompID and TargetCompID values belong to the same persistence session. * USERSESSION - Persistence session is created based on the persistence parameter value provided from an extension. Possible values = SOURCEIP, COOKIEINSERT,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			SSLSESSION, RULE, URLPASSIVE, CUSTOMSERVERID, DESTIP, SRCIPDESTIP, CALLID, RTSPSID, DIAMETER, FIXSESSION, USERSESSION, NONE
timeout	<Integer>	Read-write	Time period for which a persistence session is in effect. Default value: 2 Minimum value = 0 Maximum value = 1440
persistencebackup	<String>	Read-write	Backup persistence type for the virtual server. Becomes operational if the primary persistence mechanism fails. Possible values = SOURCEIP, NONE
backuppersistencetimeout	<Integer>	Read-write	Time period for which backup persistence is in effect. Default value: 2 Minimum value = 2

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum value = 1440
lbmethod	<String>	Read-write	Load balancing method. The available settings function as follows: * ROUNDROBIN - Distribute requests in rotation, regardless of the load. Weights can be assigned to services to enforce weighted round robin distribution. * LEASTCONNECTION (default) - Select the service with the fewest connections. * LEASTRESPONSETIME - Select the service with the lowest average response time. * LEASTBANDWIDTH - Select the service currently handling the least traffic.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			* LEASTPACKETS - Select the service currently serving the lowest number of packets per second. * CUSTOMLOAD - Base service selection on the SNMP metrics obtained by custom load monitors. * LRTM - Select the service with the lowest response time. Response times are learned through monitoring probes. This method also takes the number of active connections into account. Also available are a number of hashing methods, in which the appliance extracts a predetermined portion of the request, creates a hash of the portion, and then checks whether any previous requests

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			had the same hash value. If it finds a match, it forwards the request to the service that served those previous requests. Following are the hashing methods: * URLHASH - Create a hash of the request URL (or part of the URL). * DOMAINHASH - Create a hash of the domain name in the request (or part of the domain name). The domain name is taken from either the URL or the Host header. If the domain name appears in both locations, the URL is preferred. If the request does not contain a domain name, the load balancing method defaults to LEASTCONNECTION.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			* DESTINATIONIPHASH - Create a hash of the destination IP address in the IP header. * SOURCEIPHASH - Create a hash of the source IP address in the IP header. * TOKEN - Extract a token from the request, create a hash of the token, and then select the service to which any previous requests with the same token hash value were sent. * SRCIPDESTIPHASH - Create a hash of the string obtained by concatenating the source IP address and destination IP address in the IP header.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			* SRCIPSRCPORTHASH - Create a hash of the source IP address and source port in the IP header. * CALLIDHASH - Create a hash of the SIP Call-ID header. * USER_TOKEN - Same as TOKEN LB method but token needs to be provided from an extension. * LEASTLLMTOKENLATENCY - Select the service with the least LLM token latency. Default value: LEASTCONNECTION Possible values = ROUNDROBIN, LEASTCONNECTION, LEASTRESPONSETIME, URLHASH, DOMAINHASH,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			DESTINATIONIPHASH, SOURCEIPHASH, SRCIPDESTIPHASH, LEASTBANDWIDTH, LEASTPACKETS, TOKEN, SRCIPSRCPORTHASH, LRTM, CALLIDHASH, CUSTOMLOAD, LEASTREQUEST, AUDITLOGHASH, STATICPROXIMITY, USER_TOKEN, LEASTLLMTOKEN LATENCY
hashlength	<Integer>	Read-write	Number of bytes to consider for the hash value used in the URLHASH and DOMAINHASH load balancing methods. Default value: 80 Minimum value = 1 Maximum value = 4096
netmask	<String>	Read-write	IPv4 subnet mask to apply to the destination IP address or source IP address when the load balancing

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			method is DESTINATIONIPHASH or SOURCEIPHASH. Minimum length = 1
v6netmasklen	<Integer>	Read-write	Number of bits to consider in an IPv6 destination or source IP address, for creating the hash that is required by the DESTINATIONIPHASH and SOURCEIPHASH load balancing methods. Default value: 128 Minimum value = 1 Maximum value = 128
backuplbmethod	<String>	Read-write	Backup load balancing method. Becomes operational if the primary load balancing me thod fails or cannot be used. Valid only if the primary method is based on static proximity. Default value: ROUNDROBIN

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ROUNDROBIN, LEASTCONNECTION, LEASTRESPONSETIME, SOURCEIPHASH, LEASTBANDWIDTH, LEASTPACKETS, CUSTOMLOAD
aigwprofilename	<String>	Read-write	Name of the AIGW frontend profile. For the LB vserver to function as AI gateway, this parameter must be set. Once this parameter is set using add lb vserver, it cannot be unset. Minimum length = 1 Maximum length = 255
cookiename	<String>	Read-write	Use this parameter to specify the cookie name for COOKIE peristence type. It specifies the name of cookie with a maximum of 32 characters. If not specified, cookie name is internally generated.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
rule	<String>	Read-write	Expression, or name of a named expression, against which traffic is evaluated. The following requirements apply only to the Citrix ADC CLI: * If the expression includes one or more spaces, enclose the entire expression in double quotation marks. * If the expression itself includes double quotation marks, escape the quotations by using the \ character. * Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks. Default value: "none"

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
listenpolicy	<String>	Read-write	Expression identifying traffic accepted by the virtual server. Can be either an expression (for example, CLIENT.IP.DST.IN_SUBNET(192.0.2.0/24) or the name of a named expression. In the above example, the virtual server accepts all requests whose destination IP address is in the 192.0.2.0/24 subnet. Default value: "NONE"
listenpriority	<Integer>	Read-write	Integer specifying the priority of the listen policy. A higher number specifies a lower priority. If a request matches the listen policies of more than one virtual server the virtual server whose listen policy has the highest priority (the lowest priority number) accepts the request. Default value: 101 Minimum value = 0

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum value = 101
resrule	<String>	Read-write	Expression specifying which part of a server's response to use for creating rule based persistence sessions (persistence type RULE). Can be either an expression or the name of a named expression. Example: HTTP.RES.HEADER("setcookie").VALUE(0).TYPECAST_NVLIST_T('=',';').VALUE("server1"). Default value: "none"
persistmask	<String>	Read-write	Persistence mask for IP based persistence types, for IPv4 virtual servers. Minimum length = 1
v6persistmasklen	<Integer>	Read-write	Persistence mask for IP based persistence types, for IPv6 virtual servers. Default value: 128 Minimum value = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum value = 128
rtspnat	<String>	Read-write	Use network address translation (NAT) for RTSP data connections. Default value: OFF Possible values = ON, OFF
m	<String>	Read-write	Redirection mode for load balancing. Available settings function as follows: * IP - Before forwarding a request to a server, change the destination IP address to the server's IP address. * MAC - Before forwarding a request to a server, change the destination MAC address to the server's MAC address. The destination IP address is not changed. MAC-based redirection mode is used mostly in firewall

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			load balancing deployments. * IPTUNNEL - Perform IP-in-IP encapsulation for client IP packets. In the outer IP headers, set the destination IP address to the IP address of the server and the source IP address to the subnet IP (SNIP). The client IP packets are not modified. Applicable to both IPv4 and IPv6 packets. * TOS - Encode the virtual server's TOS ID in the TOS field of the IP header. You can use either the IPTUNNEL or the TOS option to implement Direct Server Return (DSR). Default value: IP

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = IP, MAC, IPTUNNEL, TOS
tosid	<Integer>	Read-write	TOS ID of the virtual server. Applicable only when the load balancing redirection mode is set to TOS. Minimum value = 1 Maximum value = 63
datalength	<Integer>	Read-write	Length of the token to be extracted from the data segment of an incoming packet, for use in the token method of load balancing. The length of the token, specified in bytes, must not be greater than 24 KB. Applicable to virtual servers of type TCP. Minimum value = 1 Maximum value = 100
dataoffset	<Integer>	Read-write	Offset to be considered when extracting a token from the TCP payload. Applicable to virtual servers, of type TCP, using the token method of load balancing. Must be

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			within the first 24 KB of the TCP payload. Minimum value = 0 Maximum value = 25400
sessionless	<String>	Read-write	Perform load balancing on a per-packet basis, without establishing sessions. Recommended for load balancing of intrusion detection system (IDS) servers and scenarios involving direct server return (DSR), where session information is unnecessary. Default value: DISABLED Possible values = ENABLED, DISABLED
trofspersistence	<String>	Read-write	When value is ENABLED, Trofs persistence is honored. When value is DISABLED, Trofs persistence is not honored. Default value: ENABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ENABLED, DISABLED
state	<String>	Read-write	State of the load balancing virtual server. Default value: ENABLED Possible values = ENABLED, DISABLED
connfailover	<String>	Read-write	Mode in which the connection failover feature must operate for the virtual server. After a failover, established TCP connections and UDP packet flows are kept active and resumed on the secondary appliance. Clients remain connected to the same servers. Available settings function as follows: * STATEFUL - The primary appliance shares state information with the secondary appliance, in real time, resulting in some runtime

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			processing overhead. * STATELESS - State information is not shared, and the new primary appliance tries to re-create the packet flow on the basis of the information contained in the packets it receives. * DISABLED - Connection failover does not occur. Default value: DISABLED Possible values = DISABLED, STATEFUL, STATELESS
redirurl	<String>	Read-write	URL to which to redirect traffic if the virtual server becomes unavailable. WARNING! Make sure that the domain in the URL does not match the domain specified for a content switching policy. If it does,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			requests are continuously redirected to the unavailable virtual server. Minimum length = 1
cacheable	<String>	Read-write	Route cacheable requests to a cache redirection virtual server. The load balancing virtual server can forward requests only to a transparent cache redirection virtual server that has an IP address and port combination of *:80, so such a cache redirection virtual server must be configured on the appliance. Default value: NO Possible values = YES, NO
clttimeout	<Integer>	Read-write	Idle time, in seconds, after which a client connection is terminated. Minimum value = 0 Maximum value = 31536000

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
somethod	<String>	Read-write	Type of threshold that, when exceeded, triggers spillover. Available settings function as follows: * CONNECTION - Spillover occurs when the number of client connections exceeds the threshold. * DYNAMICCONNECTION - Spillover occurs when the number of client connections at the virtual server exceeds the sum of the maximum client (Max Clients) settings for bound services. Do not specify a spillover threshold for this setting, because the threshold is implied by the Max Clients settings of bound services. * BANDWIDTH - Spillover occurs when the bandwidth consumed by the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			virtual server's incoming and outgoing traffic exceeds the threshold. * HEALTH - Spillover occurs when the percentage of weights of the services that are UP drops below the threshold. For example, if services svc1, svc2, and svc3 are bound to a virtual server, with weights 1, 2, and 3, and the spillover threshold is 50%, spillover occurs if svc1 and svc3 or svc2 and svc3 transition to DOWN. * LLMQUOTA - Spillover occurs when the LLM token quota of all the services bound the vserver is exhausted. Do not specify a spillover threshold for this setting, because the threshold is implied

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			by the max tokens settings on the bound services. * NONE - Spillover does not occur. Possible values = CONNECTION, DYNAMICCONNECTION, BANDWIDTH, HEALTH, LLMQUOTA, NONE
sopersistence	<String>	Read-write	If spillover occurs, maintain source IP address based persistence for both primary and backup virtual servers. Default value: DISABLED Possible values = ENABLED, DISABLED
sopersistencetimeout	<Integer>	Read-write	Timeout for spillover persistence, in minutes. Default value: 2 Minimum value = 2 Maximum value = 1440
healththreshold	<Integer>	Read-write	Threshold in percent of active services

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			below which vserver state is made down. If this threshold is 0, vserver state will be up even if one bound service is up. Default value: 0 Minimum value = 0 Maximum value = 100
sothreshold	<Integer>	Read-write	Threshold at which spillover occurs. Specify an integer for the CONNECTION spillover method, a bandwidth value in kilobits per second for the BANDWIDTH method (do not enter the units), or a percentage for the HEALTH method (do not enter the percentage symbol). Minimum value = 1 Maximum value = 4294967287
sobackupaction	<String>	Read-write	Action to be performed if spillover is to take effect, but no backup chain to spillover is usable or exists.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = DROP, ACCEPT, REDIRECT
redirectportrewrite	<String>	Read-write	Rewrite the port and change the protocol to ensure successful HTTP redirects from services. Default value: DISABLED Possible values = ENABLED, DISABLED
downstateflush	<String>	Read-write	Flush all active transactions associated with a virtual server whose state transitions from UP to DOWN. Do not enable this option for applications that must complete their transactions. Default value: ENABLED Possible values = ENABLED, DISABLED
backupvserver	<String>	Read-write	Name of the backup virtual server to which to forward requests if the primary virtual server goes DOWN or

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			reaches its spillover threshold. Minimum length = 1
disableprimaryondown	<String>	Read-write	If the primary virtual server goes down, do not allow it to return to primary status until manually enabled. Default value: DISABLED Possible values = ENABLED, DISABLED
insertvserveripport	<String>	Read-write	Insert an HTTP header, whose value is the IP address and port number of the virtual server, before forwarding a request to the server. The format of the header is <vipHeader>: <virtual server IP address>_<port number >, where vipHeader is the name that you specify for the header. If the virtual server has an IPv6 address, the address in the header is enclosed in brackets ([and]) to separate it from the port number. If you have mapped an IPv4

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			address to a virtual server's IPv6 address, the value of this parameter determines which IP address is inserted in the header, as follows: * VIPADDR - Insert the IP address of the virtual server in the HTTP header regardless of whether the virtual server has an IPv4 address or an IPv6 address. A mapped IPv4 address, if configured, is ignored. * V6TOV4MAPPING - Insert the IPv4 address that is mapped to the virtual server's IPv6 address. If a mapped IPv4 address is not configured, insert the IPv6 address. * OFF - Disable header insertion.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = OFF, VIPADDR, V6TOV4MAPPING
vipheader	<String>	Read-write	Name for the inserted header. The default name is vip-header. Minimum length = 1
authenticationhost	<String>	Read-write	Fully qualified domain name (FQDN) of the authentication virtual server to which the user must be redirected for authentication. Make sure that the Authentication parameter is set to ENABLED. Minimum length = 3 Maximum length = 252
authentication	<String>	Read-write	Enable or disable user authentication. Default value: OFF Possible values = ON, OFF
authn401	<String>	Read-write	Enable or disable user authentication with HTTP 401 responses. Default value: OFF

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ON, OFF
authnvsname	<String>	Read-write	Name of an authentication virtual server with which to authenticate users. Minimum length = 1 Maximum length = 252
push	<String>	Read-write	Process traffic with the push virtual server that is bound to this load balancing virtual server. Default value: DISABLED Possible values = ENABLED, DISABLED
pushvserver	<String>	Read-write	Name of the load balancing virtual server, of type PUSH or SSL_PUSH, to which the server pushes updates received on the load balancing virtual server that you are configuring. Minimum length = 1
pushlabel	<String>	Read-write	Expression for extracting a label from the server's response. Can be either an expression

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			or the name of a named expression. Default value: "none"
pushmulticlients	<String>	Read-write	Allow multiple Web 2.0 connections from the same client to connect to the virtual server and expect updates. Default value: NO Possible values = YES, NO
tcpprofilename	<String>	Read-write	Name of the TCP profile whose settings are to be applied to the virtual server. Minimum length = 1 Maximum length = 127
httpprofilename	<String>	Read-write	Name of the HTTP profile whose settings are to be applied to the virtual server. Minimum length = 1 Maximum length = 127
dbprofilename	<String>	Read-write	Name of the DB profile whose settings are to be

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			applied to the virtual server. Minimum length = 1 Maximum length = 127
mcpprofilename	<String>	Read-write	Name of the MCP profile to attach to this lb vserver. Enables MCP protocol processing.
comment	<String>	Read-write	Any comments that you might want to associate with the virtual server.
l2conn	<String>	Read-write	Use Layer 2 parameters (channel number, MAC address, and VLAN ID) in addition to the 4-tuple (<source IP>:<source port>::<destination IP>:<destination port>) that is used to identify a connection. Allows multiple TCP and non-TCP connections with the same 4-tuple to co-exist on the Citrix ADC. Possible values = ON, OFF
oracleserverversion	<String>	Read-write	Oracle server version.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: 10G Possible values = 10G, 11G
mssqlserverversion	<String>	Read-write	For a load balancing virtual server of type MSSQL, the Microsoft SQL Server version. Set this parameter if you expect some clients to run a version different from the version of the database. This setting provides compatibility between the client-side and server-side connections by ensuring that all communication conforms to the server's version. Default value: 2008R2 Possible values = 70, 2000, 2000SP1, 2005, 2008, 2008R2, 2012, 2014
mysqlprotocolversion	<Integer>	Read-write	MySQL protocol version that the virtual server advertises to clients.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
mysqlserverversion	<String>	Read-write	MySQL server version string that the virtual server advertises to clients. Minimum length = 1 Maximum length = 31
mysqlcharacterset	<Integer>	Read-write	Character set that the virtual server advertises to clients.
mysqlservercapabilities	<Integer>	Read-write	Server capabilities that the virtual server advertises to clients.
appflowlog	<String>	Read-write	Apply AppFlow logging to the virtual server. Default value: ENABLED Possible values = ENABLED, DISABLED
netprofile	<String>	Read-write	Name of the network profile to associate with the virtual server. If you set this parameter, the virtual server uses only the IP addresses in the network profile as source IP addresses when initiating connections with servers.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum length = 1 Maximum length = 127
icmpvsrresponse	<String>	Read-write	How the Citrix ADC responds to ping requests received for an IP address that is common to one or more virtual servers. Available settings function as follows: * If set to PASSIVE on all the virtual servers that share the IP address, the appliance always responds to the ping requests. * If set to ACTIVE on all the virtual servers that share the IP address, the appliance responds to the ping requests if at least one of the virtual servers is UP. Otherwise, the appliance does not respond. * If set to ACTIVE on some virtual servers and PASSIVE on the others, the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			appliance responds if at least one virtual server with the ACTIVE setting is UP. Otherwise, the appliance does not respond. Note: This parameter is available at the virtual server level. A similar parameter, ICMP Response, is available at the IP address level, for IPv4 addresses of type VIP. To set that parameter, use the add ip command in the CLI or the Create IP dialog box in the GUI. Default value: PASSIVE Possible values = PASSIVE, ACTIVE
rhistate	<String>	Read-write	Route Health Injection (RHI) functionality of the NetSaler appliance for advertising the route of the VIP address associated with the virtual

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			server. When Vserver RHI Level (RHI) parameter is set to VSVR_CNTRLD, the following are different RHI behaviors for the VIP address on the basis of RHIstate (RHI STATE) settings on the virtual servers associated with the VIP address: * If you set RHI STATE to PASSIVE on all virtual servers, the Citrix ADC always advertises the route for the VIP address. * If you set RHI STATE to ACTIVE on all virtual servers, the Citrix ADC advertises the route for the VIP address if at least one of the associated virtual servers is in UP state. * If you set RHI STATE to ACTIVE on some and PASSIVE on others,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			the Citrix ADC advertises the route for the VIP address if at least one of the associated virtual servers, whose RHI STATE set to ACTIVE, is in UP state. Default value: PASSIVE Possible values = PASSIVE, ACTIVE
newservicerequest	<Integer>	Read-write	Number of requests, or percentage of the load on existing services, by which to increase the load on a new service at each interval in slow-start mode. A non-zero value indicates that slow-start is applicable. A zero value indicates that the global RR startup parameter is applied. Changing the value to zero will cause services currently in slow start to take the full traffic as determined by the LB method. Subsequently, any new services added

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			will use the global RR factor. Default value: 0
newservicerequestunit	<String>	Read-write	Units in which to increment load at each interval in slow-start mode. Default value: PER_SECOND Possible values = PER_SECOND, PERCENT
newservicerequestincrementinterval	<Integer>	Read-write	Interval, in seconds, between successive increments in the load on a new service or a service whose state has just changed from DOWN to UP. A value of 0 (zero) specifies manual slow start. Default value: 0 Minimum value = 0 Maximum value = 3600
minautoscalemembers	<Integer>	Read-write	Minimum number of members expected to be present when vserver is used in Autoscale. Default value: 0

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum value = 0 Maximum value = 5000
maxautoscalemembers	<Integer>	Read-write	Maximum number of members expected to be present when vserver is used in Autoscale. Default value: 0 Minimum value = 0 Maximum value = 5000
persistavpno	<Integer[]>	Read-write	Persist AVP number for Diameter Persistency. In case this AVP is not defined in Base RFC 3588 and it is nested inside a Grouped AVP, define a sequence of AVP numbers (max 3) in order of parent to child. So say persist AVP number X is nested inside AVP Y which is nested in Z, then define the list as Z Y X. Minimum value = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
skippersistency	<String>	Read-write	This argument decides the behavior incase the service which is selected from an existing persistence session has reached threshold. Default value: None Possible values = Bypass, ReLb, None
td	<Integer>	Read-write	Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0. Minimum value = 0 Maximum value = 4094
authnprofile	<String>	Read-write	Name of the authentication profile to be used when authentication is turned on.
macmoderetainvlan	<String>	Read-write	This option is used to retain vlan information of incoming packet

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			when macmode is enabled. Default value: DISABLED Possible values = ENABLED, DISABLED
dbslb	<String>	Read-write	Enable database specific load balancing for MySQL and MSSQL service types. Default value: DISABLED Possible values = ENABLED, DISABLED
dns64	<String>	Read-write	This argument is for enabling/disabling the dns64 on lbvserver. Possible values = ENABLED, DISABLED
bypassaaaa	<String>	Read-write	If this option is enabled while resolving DNS64 query AAAA queries are not sent to back end dns server. Default value: NO Possible values = YES, NO

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
recursionavailable	<String>	Read-write	When set to YES, this option causes the DNS replies from this vserver to have the RA bit turned on. Typically one would set this option to YES, when the vserver is load balancing a set of DNS servers thatsupport recursive queries. Default value: NO Possible values = YES, NO
processlocal	<String>	Read-write	By turning on this option packets destined to a vserver in a cluster will not under go any steering. Turn this option for single packet request response mode or when the upstream device is performing a proper RSS for connection based distribution. Default value: DISABLED Possible values = ENABLED, DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
dnsprofilename	<String>	Read-write	Name of the DNS profile to be associated with the VServer. DNS profile properties will be applied to the transactions processed by a VServer. This parameter is valid only for DNS and DNS-TCP VServers. Minimum length = 1 Maximum length = 127
lbprofilename	<String>	Read-write	Name of the LB profile which is associated to the vserver.
redirectfromport	<Integer>	Read-write	Port number for the virtual server, from which we absorb the traffic for http redirect. Minimum value = 1 Range 1 - 65535 * in CLI is represented as 65535 in NITRO API
httpsredirecturl	<String>	Read-write	URL to which all HTTP traffic received on the port specified in the -redirectFromPort

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			parameter is redirected.
retainconnectionsoncluster	<String>	Read-write	This option enables you to retain existing connections on a node joining a Cluster system or when a node is being configured for passive timeout. By default, this option is disabled. Default value: NO Possible values = YES, NO
adfsproxyprofile	<String>	Read-write	Name of the adfsProxy profile to be used to support ADFSPIP protocol for ADFS servers.
tcpprobeport	<Integer>	Read-write	Port number for external TCP probe. NetScaler provides support for external TCP health check of the vserver status over the selected port. This option is only supported for vservers assigned with an IPAddress or ipset. Minimum value = 1 Range 1 - 65535

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			* in CLI is represented as 65535 in NITRO API
quicprofilename	<String>	Read-write	Name of QUIC profile which will be attached to the VServer. Minimum length = 1 Maximum length = 255
quicbridgeprofilename	<String>	Read-write	Name of the QUIC Bridge profile whose settings are to be applied to the virtual server. Minimum length = 1 Maximum length = 127
probeprotocol	<String>	Read-write	Citrix ADC provides support for external health check of the vserver status. Select HTTP or TCP probes for healthcheck. Possible values = TCP, HTTP
probesuccessresponsecode	<String>	Read-write	HTTP code to return in SUCCESS case. Default value: "200 OK"

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum length = 1 Maximum length = 64
probeport	<Integer>	Read-write	Citrix ADC provides support for external health check of the vserver status. Select port for HTTP/ TCP monitring. Default value: 0 Range 1 - 65535 * in CLI is represented as 65535 in NITRO API
toggleorder	<String>	Read-write	Configure this option to toggle order preference. Default value: ASCENDING Possible values = ASCENDING, DESCENDING
orderthreshold	<Integer>	Read-write	This option is used to to specify the threshold of minimum number of services to be UP in an order, for it to be considered in Lb decision. Default value: 0

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum value = 0 Maximum value = 100
apiprofile	<String>	Read-write	The API profile where one or more API specs are bounded to. Minimum length = 1
dnsoverhttps	<String>	Read-write	This option is used to enable/disable DNS over HTTPS (DoH) processing. Default value: DISABLED Possible values = ENABLED, DISABLED
wasmmodule	<String>	Read-write	Name of the WASM module to assign to this virtual server.
servicename	<String>	Read-write	Service to bind to the virtual server. Minimum length = 1
weight	<Integer>	Read-write	Weight to assign to the specified service. Minimum value = 1 Maximum value = 100
order	<Integer>	Read-write	Order number to be assigned to the service when it is

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			bound to the lb vserver. Minimum value = 1 Maximum value = 8192
redirurlflags	<Boolean>	Read-write	The redirect URL to be unset.
newname	<String>	Read-write	New name for the virtual server. Minimum length = 1
value	<String>	Read-only	SSL status. Possible values = Certkey/ Certkeybundle/Vault not bound/Cert-store not usable, SSL feature disabled
ipmapping	<String>	Read-only	The permanent mapping for the V6 Address.
ngname	<String>	Read-only	Nodegroup name to which this lbvsever belongs to.
type	<String>	Read-only	Type of LB vserver. Possible values = CONTENT, ADDRESS
curstate	<String>	Read-only	Current LB vserver state.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = UP, DOWN, UNKNOWN, BUSY, OUT OF SERVICE, GOING OUT OF SERVICE, DOWN WHEN GOING OUT OF SERVICE, NS_EMPTY_STR, Unknown, DISABLED
effectivestate	<String>	Read-only	Effective state of the LB vserver , based on the state of backup vservers. Possible values = UP, DOWN, UNKNOWN, BUSY, OUT OF SERVICE, GOING OUT OF SERVICE, DOWN WHEN GOING OUT OF SERVICE, NS_EMPTY_STR, Unknown, DISABLED
status	<Integer>	Read-only	Current status of the lb vserver. During the initial phase if the configured lb method is not round robin , the vserver will adopt round robin to distribute traffic for a predefined number of requests.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
lbrrreason	<Integer>	Read-only	Reason why a vserver is in RR. The following are the reasons: 1 - MEP is DOWN (GSLB) 2 - LB method has changed 3 - Bound service's state changed to UP 4 - A new service is bound 5 - Startup RR factor has changed 6 - LB feature is enabled 7 - Load monitor is not active on a service 8 - Vserver is Enabled 9 - SSL feature is Enabled 10 - All bound services have reached threshold. Using effective state to load balance (GSLB)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			11 - Primary state of bound services are not UP. Using effective state to load balance (GSLB) 12 - No LB decision can be made as all bound services have either reached threshold or are not UP (GSLB) 13 - All load monitors are active .
redirect	<String>	Read-only	Cache redirect type. Possible values = CACHE, POLICY, ORIGIN
precedence	<String>	Read-only	Precedence. Possible values = RULE, URL
homepage	<String>	Read-only	Home page.
dnsvservername	<String>	Read-only	DNS vserver name.
domain	<String>	Read-only	Domain.
cachevserver	<String>	Read-only	Cache virtual server.
health	<Integer>	Read-only	Health of vserver based on percentage of weights of active svcs/all svcs. This

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			does not consider administratively disabled svcs.
ruletype	<Integer>	Read-only	Rule type.
groupname	<String>	Read-only	LB group to which the lb vserver is to be bound.
cookiedomain	<String>	Read-only	Domain name to be used in the set cookie header in case of cookie persistence.
map	<String>	Read-only	Map. Possible values = ON, OFF
gt2gb	<String>	Read-only	Allow for greater than 2 GB transactions on this vserver. Default value: DISABLED Possible values = ENABLED, DISABLED
consolidatedlconn	<String>	Read-only	Use consolidated stats for LeastConnection. Default value: GLOBAL Possible values = GLOBAL, NO, YES

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
consolidatedlconngbl	<String>	Read-only	Fetches Global setting. Possible values = YES, NO
thresholdvalue	<Integer>	Read-only	Tells whether threshold exceeded for this service participating in CUSTOMLB.
bindpoint	<String>	Read-only	The bindpoint to which the policy is bound. Possible values = REQUEST, RESPONSE, MQTT_JUMBO_REQ
version	<Integer>	Read-only	Cookie version.
totalservices	<Integer>	Read-only	Total number of services bound to the vserver.
activeservices	<Integer>	Read-only	Total number of active services bound to the vserver.
statechangetimesec	<String>	Read-only	Time when last state change happened. Seconds part.
statechangetimeseconds	<Integer>	Read-only	Time when last state change happened. Seconds part.
statechangetimemsec	<Integer>	Read-only	Time at which last state change

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			happened. Milliseconds part.
tickssincelaststatechange	<Integer>	Read-only	Time in 10 millisecond ticks since the last state change.
isgslb	<Boolean>	Read-only	This field is set to true if it is a GSLBVserver.
vsvrdynconnsothreshold	<Integer>	Read-only	Spillover threshold for dynamic connection.
backupvserverstatus	<String>	Read-only	Staus of BackUp Vserver .
nodefaultbindings	<String>	Read-only	to determine if the configuration will have default ssl CIPHER and ECC curve bindings. Default value: NO Possible values = YES, NO
currentactiveorder	<String>	Read-only	current order that takes the traffic in case service or servicegroup is bound with order.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- ENABLE
- DISABLE
- GET (ALL)
- GET
- COUNT
- RENAME

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"lbvserver":{

<b>"name":<String_value>,

</b><b>"servicetype":<String_value>,

</b>"ipv46":<String_value>,

"ippattern":<String_value>,

"ipmask":<String_value>,

"port":<Integer_value>,

"ipset":<String_value>,

"range":<Integer_value>,

"persistencetype":<String_value>,

"timeout":<Integer_value>,

"persistencebackup":<String_value>,

"backuppersistencetimeout":<Integer_value>,

"lbmethod":<String_value>,

"hashlength":<Integer_value>,

"netmask":<String_value>,

"v6netmasklen":<Integer_value>,
```

```
"backuplbmethod":<String_value>,

"aigwprofilename":<String_value>,

"cookiename":<String_value>,

"rule":<String_value>,

"listenpolicy":<String_value>,

"listenpriority":<Integer_value>,

"resrule":<String_value>,

"persistmask":<String_value>,

"v6persistmasklen":<Integer_value>,

"rtspnat":<String_value>,

"m":<String_value>,

"tosid":<Integer_value>,

"datalength":<Integer_value>,

"dataoffset":<Integer_value>,

"sessionless":<String_value>,

"trofspersistence":<String_value>,

"state":<String_value>,

"connfailover":<String_value>,

"redirurl":<String_value>,

"cacheable":<String_value>,

"clttimeout":<Integer_value>,

"somethod":<String_value>,
```

```
"sopersistence":<String_value>,

"sopersistencetimeout":<Integer_value>,

"healththreshold":<Integer_value>,

"sothreshold":<Integer_value>,

"sobackupaction":<String_value>,

"redirectportrewrite":<String_value>,

"downstateflush":<String_value>,

"backupvserver":<String_value>,

"disableprimaryondown":<String_value>,

"insertvserveripport":<String_value>,

"vipheader":<String_value>,

"authenticationhost":<String_value>,

"authentication":<String_value>,

"authn401":<String_value>,

"authnvsname":<String_value>,

"push":<String_value>,

"pushvserver":<String_value>,

"pushlabel":<String_value>,

"pushmulticlients":<String_value>,

"tcpprofilename":<String_value>,

"httpprofilename":<String_value>,

"dbprofilename":<String_value>,
```

```
"mcpprofilename":<String_value>,

"comment":<String_value>,

"l2conn":<String_value>,

"oracleserverversion":<String_value>,

"mssqlserverversion":<String_value>,

"mysqlprotocolversion":<Integer_value>,

"mysqlserverversion":<String_value>,

"mysqlcharacterset":<Integer_value>,

"mysqlservercapabilities":<Integer_value>,

"appflowlog":<String_value>,

"netprofile":<String_value>,

"icmpvsrresponse":<String_value>,

"rhistate":<String_value>,

"newservicerequest":<Integer_value>,

"newservicerequestunit":<String_value>,

"newservicerequestincrementinterval":<Integer_value>,

"minautoscalemembers":<Integer_value>,

"maxautoscalemembers":<Integer_value>,

"persistavpno":<Integer[]_value>,

"skippersistency":<String_value>,

"td":<Integer_value>,

"authnprofile":<String_value>,
```

```
"macmoderetainvlan":<String_value>,

"dbslb":<String_value>,

"dns64":<String_value>,

"bypassaaaa":<String_value>,

"recursionavailable":<String_value>,

"processlocal":<String_value>,

"dnsprofilename":<String_value>,

"lbprofilename":<String_value>,

"redirectfromport":<Integer_value>,

"httpsredirecturl":<String_value>,

"retainconnectionsoncluster":<String_value>,

"adfsproxyprofile":<String_value>,

"tcpprobeport":<Integer_value>,

"quicprofilename":<String_value>,

"quicbridgeprofilename":<String_value>,

"probeprotocol":<String_value>,

"probesuccessresponsecode":<String_value>,

"probeport":<Integer_value>,

"toggleorder":<String_value>,

"orderthreshold":<Integer_value>,

"apiprofile":<String_value>,

"dnsoverhttps":<String_value>,
```

```
"wasmmodule":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"lbvserver":{

<b>"name":<String_value>,

</b>"ipv46":<String_value>,

"ipset":<String_value>,

"ippattern":<String_value>,
```

```
"ipmask":<String_value>,

"servicename":<String_value>,

"weight":<Integer_value>,

"order":<Integer_value>,

"persistencetype":<String_value>,

"timeout":<Integer_value>,

"persistencebackup":<String_value>,

"backuppersistencetimeout":<Integer_value>,

"lbmethod":<String_value>,

"hashlength":<Integer_value>,

"netmask":<String_value>,

"v6netmasklen":<Integer_value>,

"backuplbmethod":<String_value>,

"rule":<String_value>,

"cookiename":<String_value>,

"resrule":<String_value>,

"persistmask":<String_value>,

"v6persistmasklen":<Integer_value>,

"rtspnat":<String_value>,

"m":<String_value>,

"tosid":<Integer_value>,

"datalength":<Integer_value>,
```

```
"dataoffset":<Integer_value>,

"sessionless":<String_value>,

"trofspersistence":<String_value>,

"connfailover":<String_value>,

"backupvserver":<String_value>,

"redirurl":<String_value>,

"cacheable":<String_value>,

"clttimeout":<Integer_value>,

"somethod":<String_value>,

"sothreshold":<Integer_value>,

"sopersistence":<String_value>,

"sopersistencetimeout":<Integer_value>,

"healththreshold":<Integer_value>,

"sobackupaction":<String_value>,

"redirectportrewrite":<String_value>,

"downstateflush":<String_value>,

"insertvserveripport":<String_value>,

"vipheader":<String_value>,

"disableprimaryondown":<String_value>,

"authenticationhost":<String_value>,

"authentication":<String_value>,

"authn401":<String_value>,
```

```
"authnvsname":<String_value>,

"push":<String_value>,

"pushvserver":<String_value>,

"pushlabel":<String_value>,

"pushmulticlients":<String_value>,

"listenpolicy":<String_value>,

"listenpriority":<Integer_value>,

"tcpprofilename":<String_value>,

"httpprofilename":<String_value>,

"dbprofilename":<String_value>,

"mcpprofilename":<String_value>,

"comment":<String_value>,

"l2conn":<String_value>,

"oracleserverversion":<String_value>,

"mssqlserverversion":<String_value>,

"mysqlprotocolversion":<Integer_value>,

"mysqlserverversion":<String_value>,

"mysqlcharacterset":<Integer_value>,

"mysqlservercapabilities":<Integer_value>,

"appflowlog":<String_value>,

"netprofile":<String_value>,

"icmpvsrresponse":<String_value>,
```

```
"rhistate":<String_value>,

"newservicerequest":<Integer_value>,

"newservicerequestunit":<String_value>,

"newservicerequestincrementinterval":<Integer_value>,

"minautoscalemembers":<Integer_value>,

"maxautoscalemembers":<Integer_value>,

"persistavpno":<Integer[]_value>,

"skippersistency":<String_value>,

"authnprofile":<String_value>,

"macmoderetainvlan":<String_value>,

"dbslb":<String_value>,

"dns64":<String_value>,

"bypassaaaa":<String_value>,

"recursionavailable":<String_value>,

"processlocal":<String_value>,

"dnsprofilename":<String_value>,

"lbprofilename":<String_value>,

"redirectfromport":<Integer_value>,

"httpsredirecturl":<String_value>,

"retainconnectionsoncluster":<String_value>,

"adfsproxyprofile":<String_value>,

"tcpprobeport":<Integer_value>,
```

```
"quicprofilename":<String_value>,

"quicbridgeprofilename":<String_value>,

"probeport":<Integer_value>,

"probeprotocol":<String_value>,

"probesuccessresponsecode":<String_value>,

"togglеorder":<String_value>,

"orderthreshold":<Integer_value>,

"apiprofile":<String_value>,

"dnsoverhttps":<String_value>,

"wasmmodule":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"lbvserver":{

<b>"name":<String_value>,

</b>"backupvserver":true,

"clttimeout":true,

"redirurl":true,

"redirurlflags":true,

"authn401":true,

"authentication":true,

"authenticationhost":true,

"authnvsname":true,

"pushvserver":true,

"pushlabel":true,

"tcpprofilename":true,

"httpprofilename":true,

"dbprofilename":true,

"rule":true,

"sothreshold":true,

"l2conn":true,

"mysqlprotocolversion":true,

"mysqlserverversion":true,

"mysqlcharacterset":true,

"mysqlservercapabilities":true,
```

```
"appflowlog":true,
"netprofile":true,
"icmpvsrresponse":true,
"skippersistency":true,
"minautoscalemembers":true,
"maxautoscalemembers":true,
"authnprofile":true,
"macmoderetainvlan":true,
"dbslb":true,
"dnsprofilename":true,
"lbprofilename":true,
"redirectfromport":true,
"httpsredirecturl":true,
"adfsproxyprofile":true,
"tcpprobeport":true,
"quicprofilename":true,
"quicbridgeprofilename":true,
"probeprotocol":true,
"servicename":true,
"order":true,
"apiprofile":true,
"dnsoverhttps":true,
```

```
"wasmmodule":true,

"ipset":true,

"persistencetype":true,

"timeout":true,

"persistencebackup":true,

"backuppersistencetimeout":true,

"lbmethod":true,

"hashlength":true,

"netmask":true,

"v6netmasklen":true,

"backuplbmethod":true,

"cookiename":true,

"resrule":true,

"persistmask":true,

"v6persistmasklen":true,

"rtspnat":true,

"m":true,

"tosid":true,

"datalength":true,

"dataoffset":true,

"sessionless":true,

"trofspersistence":true,
```

```
"connfailover":true,

"cacheable":true,

"somethod":true,

"sopersistence":true,

"sopersistencetimeout":true,

"healththreshold":true,

"sobackupaction":true,

"redirectportrewrite":true,

"downstateflush":true,

"insertvserveripport":true,

"vipheader":true,

"disableprimaryondown":true,

"push":true,

"pushmulticlients":true,

"listenpolicy":true,

"listenpriority":true,

"mcpprofilename":true,

"comment":true,

"oracleserverversion":true,

"mssqlserverversion":true,

"rhistate":true,

"newservicerequest":true,
```

```
"newservicerequestunit":true,

"newservicerequestincrementinterval":true,

"persistavpno":true,

"recursionavailable":true,

"retainconnectionsoncluster":true,

"probesuccessresponsecode":true,

"toggleorder":true,

"orderthreshold":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

ENABLE

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver? **action=enable HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"lbvserver":{

<b>"name":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DISABLE

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver? **action=disable HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"lbvserver":{

<b>"name":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

RENAME

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver? **action=rename HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"lbvserver":{

<b>"name":<String_value>,

</b><b>"newname":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/lbvserver? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/lbvserver? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of lbvserver resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/lbvserver? **view=summary**

Use this query-parameter to get the summary output of lbvserver resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/lbvserver? **pagesize=#no;pageno=#no**

Use this query-parameter to get the lbvserver resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "lbvserver": [ {

"name":<String_value>,

"insertvserveripport":<String_value>,

"vipheader":<String_value>,

"value":<String_value>,

"ip":<String_value>,

"ipv46":<String_value>,

"ippattern":<String_value>,

"ipmask":<String_value>,

"listenpolicy":<String_value>,

"listenpriority":<Integer_value>,

"ipmapping":<String_value>,

"port":<Integer_value>,

"ipset":<String_value>,

"range":<Integer_value>,

"servicetype":<String_value>,

"ngname":<String_value>,
```

```
"type":<String_value>,

"curstate":<String_value>,

"effectivestate":<String_value>,

"status":<Integer_value>,

"lbrrreason":<Integer_value>,

"redirect":<String_value>,

"precedence":<String_value>,

"redirurl":<String_value>,

"authentication":<String_value>,

"authn401":<String_value>,

"authnvsname":<String_value>,

"homepage":<String_value>,

"dnsvservername":<String_value>,

"domain":<String_value>,

"servicename":<String_value>,

"weight":<Integer_value>,

"cachevserver":<String_value>,

"backupvserver":<String_value>,

"clttimeout":<Integer_value>,

"somethod":<String_value>,

"sopersistence":<String_value>,

"sopersistencetimeout":<Integer_value>,
```

```
"healththreshold":<Integer_value>,

"sothreshold":<Integer_value>,

"sobackupaction":<String_value>,

"lbmethod":<String_value>,

"backuplbmethod":<String_value>,

"hashlength":<Integer_value>,

"dataoffset":<Integer_value>,

"health":<Integer_value>,

"datalength":<Integer_value>,

"netmask":<String_value>,

"v6netmasklen":<Integer_value>,

"rule":<String_value>,

"resrule":<String_value>,

"ruletype":<Integer_value>,

"groupname":<String_value>,

"m":<String_value>,

"tosid":<Integer_value>,

"persistencetype":<String_value>,

"timeout":<Integer_value>,

"cookiedomain":<String_value>,

"persistmask":<String_value>,

"v6persistmasklen":<Integer_value>,
```

```
"persistencebackup":<String_value>,

"backuppersistencetimeout":<Integer_value>,

"cacheable":<String_value>,

"rtspnat":<String_value>,

"sessionless":<String_value>,

"trofspersistence":<String_value>,

"map":<String_value>,

"connfailover":<String_value>,

"redirectportrewrite":<String_value>,

"downstateflush":<String_value>,

"disableprimaryondown":<String_value>,

"gt2gb":<String_value>,

"consolidatedlconn":<String_value>,

"consolidatedlconngbl":<String_value>,

"thresholdvalue":<Integer_value>,

"bindpoint":<String_value>,

"cookiename":<String_value>,

"version":<Integer_value>,

"totalservices":<Integer_value>,

"activeservices":<Integer_value>,

"statechangetimesec":<String_value>,

"statechangetimeseconds":<Integer_value>,
```

```
"statechangetimemsec":<Integer_value>,

"tickssincelaststatechange":<Integer_value>,

"authenticationhost":<String_value>,

"push":<String_value>,

"pushvserver":<String_value>,

"pushlabel":<String_value>,

"pushmulticlients":<String_value>,

"tcpprofilename":<String_value>,

"httpprofilename":<String_value>,

"dbprofilename":<String_value>,

"aigwprofilename":<String_value>,

"mcpprofilename":<String_value>,

"comment":<String_value>,

"l2conn":<String_value>,

"oracleserverversion":<String_value>,

"mssqlserverversion":<String_value>,

"mysqlprotocolversion":<Integer_value>,

"mysqlserverversion":<String_value>,

"mysqlcharacterset":<Integer_value>,

"mysqlservercapabilities":<Integer_value>,

"appflowlog":<String_value>,

"netprofile":<String_value>,
```

```
"isgslb":<Boolean_value>,

"icmpvsrresponse":<String_value>,

"rhistate":<String_value>,

"newservicerequest":<Integer_value>,

"newservicerequestunit":<String_value>,

"newservicerequestincrementinterval":<Integer_value>,

"persistavpno":<Integer[]_value>,

"skippersistency":<String_value>,

"td":<Integer_value>,

"minautoscalemembers":<Integer_value>,

"maxautoscalemembers":<Integer_value>,

"authnprofile":<String_value>,

"macmoderetainvlan":<String_value>,

"dbslb":<String_value>,

"dns64":<String_value>,

"bypassaaaa":<String_value>,

"recursionavailable":<String_value>,

"processlocal":<String_value>,

"vsvrdynconnsothreshold":<Integer_value>,

"backupvserverstatus":<String_value>,

"dnsprofilename":<String_value>,

"lbprofilename":<String_value>,
```

```
"redirectfromport":<Integer_value>,

"httpsredirecturl":<String_value>,

"retainconnectionsoncluster":<String_value>,

"nodefaultbindings":<String_value>,

"adfsproxyprofile":<String_value>,

"tcpprobeport":<Integer_value>,

"quicbridgeprofilename":<String_value>,

"probeprotocol":<String_value>,

"probeport":<Integer_value>,

"probesuccessresponsecode":<String_value>,

"quicprofilename":<String_value>,

"order":<Integer_value>,

"toggleorder":<String_value>,

"orderthreshold":<Integer_value>,

"currentactiveorder":<String_value>,

"apiprofile":<String_value>,

"dnsoverhttps":<String_value>,

"wasmmodule":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/lbvserver/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/lbvserver/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of lbvserver resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lbvserver": [ {

"name":<String_value>,

"insertvserveripport":<String_value>,

"vipheader":<String_value>,

"value":<String_value>,
```

```
"ip":<String_value>,

"ipv46":<String_value>,

"ippattern":<String_value>,

"ipmask":<String_value>,

"listenpolicy":<String_value>,

"listenpriority":<Integer_value>,

"ipmapping":<String_value>,

"port":<Integer_value>,

"ipset":<String_value>,

"range":<Integer_value>,

"servicetype":<String_value>,

"ngname":<String_value>,

"type":<String_value>,

"curstate":<String_value>,

"effectivestate":<String_value>,

"status":<Integer_value>,

"lbrrreason":<Integer_value>,

"redirect":<String_value>,

"precedence":<String_value>,

"redirurl":<String_value>,

"authentication":<String_value>,

"authn401":<String_value>,
```

```
"authnvsname":<String_value>,

"homepage":<String_value>,

"dnsvservername":<String_value>,

"domain":<String_value>,

"servicename":<String_value>,

"weight":<Integer_value>,

"cachevserver":<String_value>,

"backupvserver":<String_value>,

"clttimeout":<Integer_value>,

"somethod":<String_value>,

"sopersistence":<String_value>,

"sopersistencetimeout":<Integer_value>,

"healththreshold":<Integer_value>,

"sothreshold":<Integer_value>,

"sobackupaction":<String_value>,

"lbmethod":<String_value>,

"backuplbmethod":<String_value>,

"hashlength":<Integer_value>,

"dataoffset":<Integer_value>,

"health":<Integer_value>,

"datalength":<Integer_value>,

"netmask":<String_value>,
```

```
"v6netmasklen":<Integer_value>,

"rule":<String_value>,

"resrule":<String_value>,

"ruletype":<Integer_value>,

"groupname":<String_value>,

"m":<String_value>,

"tosid":<Integer_value>,

"persistencetype":<String_value>,

"timeout":<Integer_value>,

"cookiedomain":<String_value>,

"persistmask":<String_value>,

"v6persistmasklen":<Integer_value>,

"persistencebackup":<String_value>,

"backuppersistencetimeout":<Integer_value>,

"cacheable":<String_value>,

"rtspnat":<String_value>,

"sessionless":<String_value>,

"trofspersistence":<String_value>,

"map":<String_value>,

"connfailover":<String_value>,

"redirectportrewrite":<String_value>,

"downstateflush":<String_value>,
```

```
"disableprimaryondown":<String_value>,

"gt2gb":<String_value>,

"consolidatedlconn":<String_value>,

"consolidatedlconngbl":<String_value>,

"thresholdvalue":<Integer_value>,

"bindpoint":<String_value>,

"cookiename":<String_value>,

"version":<Integer_value>,

"totalservices":<Integer_value>,

"activeservices":<Integer_value>,

"statechangetimesec":<String_value>,

"statechangetimeseconds":<Integer_value>,

"statechangetimemsec":<Integer_value>,

"tickssincelaststatechange":<Integer_value>,

"authenticationhost":<String_value>,

"push":<String_value>,

"pushvserver":<String_value>,

"pushlabel":<String_value>,

"pushmulticlients":<String_value>,

"tcpprofilename":<String_value>,

"httpprofilename":<String_value>,

"dbprofilename":<String_value>,
```

```
"aigwprofilename":<String_value>,

"mcpprofilename":<String_value>,

"comment":<String_value>,

"l2conn":<String_value>,

"oracleserverversion":<String_value>,

"mssqlserverversion":<String_value>,

"mysqlprotocolversion":<Integer_value>,

"mysqlserverversion":<String_value>,

"mysqlcharacterset":<Integer_value>,

"mysqlservercapabilities":<Integer_value>,

"appflowlog":<String_value>,

"netprofile":<String_value>,

"isgslb":<Boolean_value>,

"icmpvsrresponse":<String_value>,

"rhistate":<String_value>,

"newservicerequest":<Integer_value>,

"newservicerequestunit":<String_value>,

"newservicerequestincrementinterval":<Integer_value>,

"persistavpno":<Integer[]_value>,

"skippersistency":<String_value>,

"td":<Integer_value>,

"minautoscalemembers":<Integer_value>,
```

```
"maxautoscalemembers":<Integer_value>,

"authnprofile":<String_value>,

"macmoderetainvlan":<String_value>,

"dbslb":<String_value>,

"dns64":<String_value>,

"bypassaaaa":<String_value>,

"recursionavailable":<String_value>,

"processlocal":<String_value>,

"vsvrdynconnsothreshold":<Integer_value>,

"backupvserverstatus":<String_value>,

"dnsprofilename":<String_value>,

"lbprofilename":<String_value>,

"redirectfromport":<Integer_value>,

"httpsredirecturl":<String_value>,

"retainconnectionsoncluster":<String_value>,

"nodefaultbindings":<String_value>,

"adfsproxyprofile":<String_value>,

"tcpprobeport":<Integer_value>,

"quicbridgeprofilename":<String_value>,

"probeprotocol":<String_value>,

"probeport":<Integer_value>,

"probesuccessresponsecode":<String_value>,
```

```
"quicprofilename":<String_value>,

"order":<Integer_value>,

"toggleorder":<String_value>,

"orderthreshold":<Integer_value>,

"currentactiveorder":<String_value>,

"apiprofile":<String_value>,

"dnsoverhttps":<String_value>,

"wasmmodule":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "lbvserver": [ { "__count": "#no"} ] }
```

lbvserver_analyticsprofile_binding

Binding object showing the analyticsprofile that can be bound to lbvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the virtual server. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at sign (@), equal sign (=), and hyphen (-) characters. Can be changed after the virtual server is created.

CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my vserver" or 'my vserver'). .

Minimum length = 1

Minimum value = 1

Maximum value = 8192

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/lbvserver_analyticsprofile_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"lbvserver_analyticsprofile_binding":{

<b>"name":<String_value>,

</b>"analyticsprofile":<String_value>,

"order":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_analyticsprofile_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ lbvserver_analyticsprofile_binding/ name_value<String> ? **args=analyticsprofile: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_analyticsprofile_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/

lbvserver_analyticsprofile_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of lbvserver_analyticsprofile_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_analyticsprofile_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the lbvserver_analyticsprofile_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lbvserver_analyticsprofile_binding": [ {

"name":<String_value>,

"analyticsprofile":<String_value>,

"order":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_analyticsprofile_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_analyticsprofile_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lbvserver_analyticsprofile_binding": [ {

"name":<String_value>,

"analyticsprofile":<String_value>,

"order":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_analyticsprofile_binding/name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"lbvserver_analyticsprofile_binding": [ { "__count": "#no"} ] }
```

lbvserver_appflowpolicy_binding

Binding object showing the appflowpolicy that can be bound to lbvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
gotopriorityexpression	<String>	Read-write	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
invoke	<Boolean>	Read-write	Invoke policies bound to a virtual server or policy label.
policyname	<String>	Read-write	Name of the policy bound to the LB vserver.
labeltype	<String>	Read-write	The invocation type. Possible values = reqvserver,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			resvserver, policylabel
priority	<Integer>	Read-write	Priority.
bindpoint	<String>	Read-write	The bindpoint to which the policy is bound. Possible values = REQUEST, RESPONSE, MQTT_JUMBO_REQ
name	<String>	Read-write	Name for the virtual server. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at sign (@), equal sign (=), and hyphen (-) characters. Can be changed after the virtual server is created.

CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my vserver" or 'my vserver'). .

Minimum length = 1

Minimum value = 1

Maximum value = 8192

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/lbvserver_appflowpolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"lbvserver_appflowpolicy_binding":{

<b>"name":<String_value>,

</b>"policyname":<String_value>,

"priority":<Integer_value>,

"gotopriorityexpression":<String_value>,

"bindpoint":<String_value>,

"invoke":<Boolean_value>,

"labeltype":<String_value>,

"labelname":<String_value>,

"order":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_appflowpolicy_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ lbvserver_appflowpolicy_binding/ name_value<String> ? **args=policyname: <String_value> ,bindpoint: <String_value> ,priority: <Integer_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_appflowpolicy_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ lbvserver_appflowpolicy_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of lbvserver_appflowpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_appflowpolicy_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the lbvserver_appflowpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lbvserver_appflowpolicy_binding": [ {

"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>,

"policyname":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"bindpoint":<String_value>,

"name":<String_value>,

"order":<Integer_value>,

"labelname":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_appflowpolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_appflowpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lbvserver_appflowpolicy_binding": [ {

"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>,

"policyname":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"bindpoint":<String_value>,

"name":<String_value>,

"order":<Integer_value>,

"labelname":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_appflowpolicy_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"lbvserver_appflowpolicy_binding": [ { "__count": "#no"} ] }
```

lbvserver_appfwpolicy_binding

Binding object showing the appfwpolicy that can be bound to lbvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
policyname	<String>	Read-write	Name of the policy bound to the LB vserver.
invoke	<Boolean>	Read-write	Invoke policies bound to a virtual server or policy label.
gotopriorityexpression	<String>	Read-write	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
labelname	<String>	Read-write	Name of the label invoked.
order	<Integer>	Read-write	Integer specifying the order of the service. A larger

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			number specifies a lower order. Defines the order of the service relative to the other services in the load balancing vserver's bindings. Determines the priority given to the service among all the services bound. Minimum value = 1 Maximum value = 8192
name	<String>	Read-write	Name for the virtual server. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at sign (@), equal sign (=), and hyphen (-) characters. Can be changed after the virtual server is created.

CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my vserver" or 'my vserver'). .

Minimum length = 1

Possible values = REQUEST, RESPONSE, MQTT_JUMBO_REQ

Possible values = reqvserver, resvserver, policylabel

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/lbvserver_appfwpolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"lbvserver_appfwpolicy_binding":{

<b>"name":<String_value>,

</b>"policyname":<String_value>,

"priority":<Integer_value>,

"gotopriorityexpression":<String_value>,

"bindpoint":<String_value>,

"invoke":<Boolean_value>,

"labeltype":<String_value>,

"labelname":<String_value>,

"order":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_appfwpolicy_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ lbvserver_appfwpolicy_binding/ name_value<String> ? **args=policyname: <String_value> ,bindpoint: <String_value> ,priority: <Integer_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_appfwpolicy_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ lbvserver_appfwpolicy_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of lbvserver_appfwpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_appfwpolicy_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the lbvserver_appfwpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lbvserver_appfwpolicy_binding": [ {

"policyname":<String_value>,

"invoke":<Boolean_value>,

"gotopriorityexpression":<String_value>,

"labelname":<String_value>,

"order":<Integer_value>,

"name":<String_value>,

"bindpoint":<String_value>,

"priority":<Integer_value>,

"labeltype":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_appfwpolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_appfwpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lbvserver_appfwpolicy_binding": [ {

"policyname":<String_value>,

"invoke":<Boolean_value>,

"gotopriorityexpression":<String_value>,

"labelname":<String_value>,

"order":<Integer_value>,

"name":<String_value>,

"bindpoint":<String_value>,

"priority":<Integer_value>,

"labeltype":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_appfwpolicy_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"lbvserver_appfwpolicy_binding": [ { "__count": "#no"} ] }
```

lbvserver_appqoepolicy_binding

Binding object showing the appqoepolicy that can be bound to lbvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
order	<Integer>	Read-write	Integer specifying the order of the service. A larger number specifies a lower order. Defines the order of the service relative to the other services in the load balancing vserver's bindings. Determines the priority given to the service among all the services bound. Minimum value = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum value = 8192
labelname	<String>	Read-write	Name of the virtual server or user-defined policy label to invoke if the policy evaluates to TRUE.
name	<String>	Read-write	Name for the virtual server. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at sign (@), equal sign (=), and hyphen (-) characters. Can be changed after the virtual server is created.

CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my vserver" or 'my vserver'). .

Minimum length = 1

Possible values = reqvserver, resvserver, policylabel

```
</td></tr><tr><td>bindpoint

</td><td>&lt;String&gt;

</td><td>Read-write

</td><td>The bindpoint to which the policy is bound.
```

```
 <p>Possible values = REQUEST, RESPONSE, MQTT_JUMBO_REQ</p>

</td></tr><tr><td>policyname

</td><td>&lt;String&gt;

</td><td>Read-write

</td><td>Name of the policy bound to the LB vserver.

</td></tr><tr><td>invoke

</td><td>&lt;Boolean&gt;

</td><td>Read-write

</td><td>Invoke policies bound to a virtual server or policy label.

</td></tr><tr><td>gotopriorityexpression

</td><td>&lt;String&gt;

</td><td>Read-write

</td><td>Expression specifying the priority of the next policy which will
get evaluated if the current policy rule evaluates to TRUE.

</td></tr><tr><td>__count

</td><td>&lt;Double&gt;

</td><td>Read-write

</td><td>count parameter

</td></tr></tbody></table>
```

Operations

(click to see Properties)

- ADD

- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/lbvserver_appqoepolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"lbvserver_appqoepolicy_binding":{

<b>"name":<String_value>,

</b>"policyname":<String_value>,

"priority":<Integer_value>,

"gotopriorityexpression":<String_value>,

"bindpoint":<String_value>,

"invoke":<Boolean_value>,

"labeltype":<String_value>,

"labelname":<String_value>,

"order":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_appqoepolicy_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ lbvserver_appqoepolicy_binding/ name_value<String> ? **args=policyname: <String_value> ,bindpoint: <String_value> ,priority: <Integer_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_appqoepolicy_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ lbvserver_appqoepolicy_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of lbvserver_appqoepolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_appqoepolicy_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the lbvserver_appqoepolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lbvserver_appqoepolicy_binding": [ {

"order":<Integer_value>,

"labelname":<String_value>,
```

```
"name":<String_value>,

"priority":<Integer_value>,

"labeltype":<String_value>,

"bindpoint":<String_value>,

"policyname":<String_value>,

"invoke":<Boolean_value>,

"gotopriorityexpression":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_appqoepolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_appqoepolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lbvserver_appqoepolicy_binding": [ {

"order":<Integer_value>,

"labelname":<String_value>,

"name":<String_value>,

"priority":<Integer_value>,

"labeltype":<String_value>,

"bindpoint":<String_value>,

"policyname":<String_value>,

"invoke":<Boolean_value>,

"gotopriorityexpression":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_appqoepolicy_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"lbvserver_appqoepolicy_binding": [ { "__count": "#no"} ] }
```

lbvserver_auditnslogpolicy_binding

Binding object showing the auditnslogpolicy that can be bound to lbvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
policyname	<String>	Read-write	Name of the policy bound to the LB vserver.
gotopriorityexpression	<String>	Read-write	Expression or other value specifying the next policy to be evaluated if the current policy evaluates to TRUE. Specify one of the following values: * NEXT - Evaluate the policy with the next higher priority number. * END - End policy evaluation. * USE_INVOCATION_RESULT - Applicable if this policy invokes another policy label. If the final goto in the invoked policy label has a value of END, the evaluation stops. If the final goto is anything other than END, the current

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			policy label performs a NEXT. * An expression that evaluates to a number. If you specify an expression, the number to which it evaluates determines the next policy to evaluate, as follows: * If the expression evaluates to a higher numbered priority, the policy with that priority is evaluated next. * If the expression evaluates to the priority of the current policy, the policy with the next higher numbered priority is evaluated next. * If the expression evaluates to a priority number that is numerically higher than the highest numbered priority, policy evaluation ends. An UNDEF event is triggered if: * The expression is invalid. * The expression evaluates to a priority number that is numerically lower than the current policy's priority. * The

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			expression evaluates to a priority number that is between the current policy's priority number (say, 30) and the highest priority number (say, 100), but does not match any configured priority number (for example, the expression evaluates to the number 85). This example assumes that the priority number increments by 10 for every successive policy, and therefore a priority number of 85 does not exist in the policy label.
invoke	<Boolean>	Read-write	Invoke policies bound to a virtual server or policy label.
name	<String>	Read-write	Name for the virtual server. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at sign (@), equal sign (=), and hyphen (-)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			characters. Can be changed after the virtual server is created.

CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my vserver" or 'my vserver'). .

Minimum length = 1

Possible values = reqvserver, resvserver, policylabel

```
</td></tr><tr><td>priority

</td><td>&lt;Integer&gt;

</td><td>Read-write

</td><td>Priority.

</td></tr><tr><td>bindpoint

</td><td>&lt;String&gt;

</td><td>Read-write

</td><td>Bind point to which to bind the policy.

 <p>Possible values = REQUEST, RESPONSE, MQTT_JUMBO_REQ</p>

</td></tr><tr><td>order

</td><td>&lt;Integer&gt;

</td><td>Read-write

 </td><td>Integer specifying the order of the service. A larger number
specifies a lower order. Defines the order of the service relative to the
other services in the load balancing vserver's bindings. Determines the
priority given to the service among all the services bound.
```

```
  <p>Minimum value =  1</p>

  <p>Maximum value =  8192</p>

 </td></tr><tr><td>labelname

 </td><td>&lt;String&gt;

 </td><td>Read-write

 </td><td>Name of the virtual server or user-defined policy label to
invoke if the policy evaluates to TRUE.

 </td></tr><tr><td>__count

 </td><td>&lt;Double&gt;

 </td><td>Read-write

 </td><td>count parameter

 </td></tr></tbody></table>
```

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/lbvserver_auditnslogpolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"lbvserver_auditnslogpolicy_binding":{

<b>"name":<String_value>,

</b>"policyname":<String_value>,

"priority":<Integer_value>,

"gotopriorityexpression":<String_value>,
```

```
"bindpoint":<String_value>,

"invoke":<Boolean_value>,

"labeltype":<String_value>,

"labelname":<String_value>,

"order":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_auditnslogpolicy_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ lbvserver_auditnslogpolicy_binding/ name_value<String> ? **args=policyname: <String_value> ,bindpoint: <String_value> ,priority: <Integer_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_auditnslogpolicy_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ lbvserver_auditnslogpolicy_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of lbvserver_auditnslogpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_auditnslogpolicy_binding/name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the lbvserver_auditnslogpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lbvserver_auditnslogpolicy_binding": [ {

"policyname":<String_value>,

"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>,

"name":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"bindpoint":<String_value>,

"order":<Integer_value>,
```

```
"labelname":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_auditnslogpolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_auditnslogpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lbvserver_auditnslogpolicy_binding": [ {

"policyname":<String_value>,

"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>,

"name":<String_value>,
```

```
"labeltype":<String_value>,

"priority":<Integer_value>,

"bindpoint":<String_value>,

"order":<Integer_value>,

"labelname":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_auditnslogpolicy_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"lbvserver_auditnslogpolicy_binding": [ { "__count": "#no"} ] }
```

lbvserver_auditsyslogpolicy_binding

Binding object showing the auditsyslogpolicy that can be bound to lbvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
invoke	<Boolean>	Read-write	Invoke policies bound to a virtual server or policy label.
gotopriorityexpression	<String>	Read-write	Expression or other value specifying the next policy to be evaluated if the current policy evaluates to TRUE. Specify one of the following values: * NEXT - Evaluate the policy with the next higher priority number. * END - End policy evaluation. * USE_INVOCATION_RESULT - Applicable if this policy invokes another policy label. If the final goto in the invoked policy label has a value of END, the evaluation stops. If the final goto is anything other than END, the current policy label performs a NEXT. * An expression that evaluates to a number. If you specify an expression, the number to which it evaluates determines the next

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			policy to evaluate, as follows: * If the expression evaluates to a higher numbered priority, the policy with that priority is evaluated next. * If the expression evaluates to the priority of the current policy, the policy with the next higher numbered priority is evaluated next. * If the expression evaluates to a priority number that is numerically higher than the highest numbered priority, policy evaluation ends. An UNDEF event is triggered if: * The expression is invalid. * The expression evaluates to a priority number that is numerically lower than the current policy's priority. * The expression evaluates to a priority number that is between the current policy's priority number (say, 30) and the highest priority number (say, 100), but does not match any configured priority

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			number (for example, the expression evaluates to the number 85). This example assumes that the priority number increments by 10 for every successive policy, and therefore a priority number of 85 does not exist in the policy label.
policyname	<String>	Read-write	Name of the policy bound to the LB vserver.
name	<String>	Read-write	Name for the virtual server. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at sign (@), equal sign (=), and hyphen (-) characters. Can be changed after the virtual server is created.

CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my vserver" or 'my vserver'). .

Minimum length = 1

Possible values = REQUEST, RESPONSE, MQTT_JUMBO_REQ

Possible values = reqvserver, resvserver, policylabel

```
 </td></tr><tr><td>order

 </td><td>&lt;Integer&gt;

 </td><td>Read-write

 </td><td>Integer specifying the order of the service. A larger number
specifies a lower order. Defines the order of the service relative to the
other services in the load balancing vserver's bindings. Determines the
priority given to the service among all the services bound.

  <p>Minimum value =  1</p>

  <p>Maximum value =  8192</p>

 </td></tr><tr><td>labelname

 </td><td>&lt;String&gt;

 </td><td>Read-write

 </td><td>Name of the virtual server or user-defined policy label to
invoke if the policy evaluates to TRUE.

 </td></tr><tr><td>__count

 </td><td>&lt;Double&gt;

 </td><td>Read-write

 </td><td>count parameter

 </td></tr></tbody></table>
```

Operations

(click to see Properties)

- ADD

- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/lbvserver_auditsyslogpolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"lbvserver_auditsyslogpolicy_binding":{

<b>"name":<String_value>,

</b>"policyname":<String_value>,

"priority":<Integer_value>,

"gotopriorityexpression":<String_value>,

"bindpoint":<String_value>,

"invoke":<Boolean_value>,

"labeltype":<String_value>,

"labelname":<String_value>,

"order":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_auditsyslogpolicy_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ lbvserver_auditsyslogpolicy_binding/ name_value<String> ? **args=policyname: <String_value> ,bindpoint: <String_value> ,priority: <Integer_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_auditsyslogpolicy_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ lbvserver_auditsyslogpolicy_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of lbvserver_auditsyslogpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_auditsyslogpolicy_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the lbvserver_auditsyslogpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lbvserver_auditsyslogpolicy_binding": [ {

"invoke":<Boolean_value>,

"gotopriorityexpression":<String_value>,
```

```
"policyname":<String_value>,

"name":<String_value>,

"bindpoint":<String_value>,

"priority":<Integer_value>,

"labeltype":<String_value>,

"order":<Integer_value>,

"labelname":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_auditsyslogpolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_auditsyslogpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lbvserver_auditsyslogpolicy_binding": [ {

"invoke":<Boolean_value>,

"gotopriorityexpression":<String_value>,

"policyname":<String_value>,

"name":<String_value>,

"bindpoint":<String_value>,

"priority":<Integer_value>,

"labeltype":<String_value>,

"order":<Integer_value>,

"labelname":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_auditsyslogpolicy_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"lbvserver_auditsyslogpolicy_binding": [ { "__count": "#no"} ] }
```

lbvserver_authorizationpolicy_binding

Binding object showing the authorizationpolicy that can be bound to lbvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
invoke	<Boolean>	Read-write	Invoke policies bound to a virtual server or policy label.
gotopriorityexpression	<String>	Read-write	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
policyname	<String>	Read-write	Name of the policy bound to the LB vserver.
order	<Integer>	Read-write	Integer specifying the order of the service. A larger number specifies a lower order. Defines the order of the service relative to the other services in the load balancing vserver's bindings. Determines the priority given to the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			service among all the services bound. Minimum value = 1 Maximum value = 8192
labelname	<String>	Read-write	Name of the label invoked.
name	<String>	Read-write	Name for the virtual server. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at sign (@), equal sign (=), and hyphen (-) characters. Can be changed after the virtual server is created.

CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my vserver" or 'my vserver'). .

Minimum length = 1

Possible values = reqvserver, resvserver, policylabel

Possible values = REQUEST, RESPONSE, MQTT_JUMBO_REQ

Operations

(click to see Properties)

- ADD

- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/lbvserver_authorizationpolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"lbvserver_authorizationpolicy_binding":{

<b>"name":<String_value>,

</b>"policyname":<String_value>,

"priority":<Integer_value>,

"gotopriorityexpression":<String_value>,

"bindpoint":<String_value>,

"invoke":<Boolean_value>,

"labeltype":<String_value>,

"labelname":<String_value>,

"order":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_authorizationpolicy_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ lbvserver_authorizationpolicy_binding/ name_value<String> ? **args=policyname: <String_value> ,bindpoint: <String_value> ,priority: <Integer_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_authorizationpolicy_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ lbvserver_authorizationpolicy_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of lbvserver_authorizationpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_authorizationpolicy_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the lbvserver_authorizationpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lbvserver_authorizationpolicy_binding": [ {

"invoke":<Boolean_value>,

"gotopriorityexpression":<String_value>,
```

```
"policyname":<String_value>,

"order":<Integer_value>,

"labelname":<String_value>,

"name":<String_value>,

"priority":<Integer_value>,

"labeltype":<String_value>,

"bindpoint":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_authorizationpolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_authorizationpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lbvserver_authorizationpolicy_binding": [ {

"invoke":<Boolean_value>,

"gotopriorityexpression":<String_value>,

"policyname":<String_value>,

"order":<Integer_value>,

"labelname":<String_value>,

"name":<String_value>,

"priority":<Integer_value>,

"labeltype":<String_value>,

"bindpoint":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_authorizationpolicy_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"lbvserver_authorizationpolicy_binding": [ { "__count": "#no"} ] }
```

lbvserver_binding

Binding object which returns the resources bound to lbvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the virtual server. If no name is provided, statistical data of all configured virtual servers is displayed. Minimum length = 1
lbvserver_transformpolicy_binding	<lbvserver_transformpolicy_binding[]>	Read-only	transformpolicy that can be bound to lbvserver.
lbvserver_videooptimizationdetectionpolicy_binding	<lbvserver_videooptimizationdetectionpolicy_binding[]>	Read-only	videooptimizationdetectionpolicy that can be bound to lbvserver.
lbvserver_spilloverpolicy_binding	<lbvserver_spilloverpolicy_binding[]>	Read-only	spilloverpolicy that can be bound to lbvserver.
lbvserver_rewritepolicy_binding	<lbvserver_rewritepolicy_binding[]>	Read-only	rewritepolicy that can be bound to lbvserver.
lbvserver_feopolicy_binding	<lbvserver_feopolicy_binding[]>	Read-only	feopolicy that can be bound to lbvserver.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
lbvserver_cachepolicy_binding	<lbvserver_cachepolicy_binding[]>	Read-only	cachepolicy that can be bound to lbvserver.
lbvserver_cmppolicy_binding	<lbvserver_cmppolicy_binding[]>	Read-only	cmppolicy that can be bound to lbvserver.
lbvserver_auditsyslogpolicy_binding	<lbvserver_auditsyslogpolicy_binding[]>	Read-only	auditsyslogpolicy that can be bound to lbvserver.
lbvserver_service_binding	<lbvserver_service_binding[]>	Read-only	service that can be bound to lbvserver.
lbvserver_videooptimizationpacingpolicy_binding	<lbvserver_videooptimizationpacingpolicy_binding[]>	Read-only	videooptimizationpacingpolicy that can be bound to lbvserver.
lbvserver_dnspolicy64_binding	<lbvserver_dnspolicy64_binding[]>	Read-only	dnspolicy64 that can be bound to lbvserver.
lbvserver_contentinspectionpolicy_binding	<lbvserver_contentinspectionpolicy_binding[]>	Read-only	contentinspectionpolicy that can be bound to lbvserver.
lbvserver_servicegroupmember_binding	<lbvserver_servicegroupmember_binding[]>	Read-only	servicegroupmember that can be bound to lbvserver.
lbvserver_appfwpolicy_binding	<lbvserver_appfwpolicy_binding[]>	Read-only	appfwpolicy that can be bound to lbvserver.
lbvserver_responderpolicy_binding	<lbvserver_responderpolicy_binding[]>	Read-only	responderpolicy that can be bound to lbvserver.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
lbvserver_appqoepolicy_binding	<lbvserver_appqoepolicy_binding[]>	Read-only	appqoepolicy that can be bound to lbvserver.
lbvserver_lbpolicy_binding	<lbvserver_lbpolicy_binding[]>	Read-only	lbpolicy that can be bound to lbvserver.
lbvserver_botpolicy_binding	<lbvserver_botpolicy_binding[]>	Read-only	botpolicy that can be bound to lbvserver.
lbvserver_auditnslogpolicy_binding	<lbvserver_auditnslogpolicy_binding[]>	Read-only	auditnslogpolicy that can be bound to lbvserver.
lbvserver_csvserver_binding	<lbvserver_csvserver_binding[]>	Read-only	csvserver that can be bound to lbvserver.
lbvserver_authorizationpolicy_binding	<lbvserver_authorizationpolicy_binding[]>	Read-only	authorizationpolicy that can be bound to lbvserver.
lbvserver_servicegroup_binding	<lbvserver_servicegroup_binding[]>	Read-only	servicegroup that can be bound to lbvserver.
lbvserver_appflowpolicy_binding	<lbvserver_appflowpolicy_binding[]>	Read-only	appflowpolicy that can be bound to lbvserver.
lbvserver_tmtrafficpolicy_binding	<lbvserver_tmtrafficpolicy_binding[]>	Read-only	tmtrafficpolicy that can be bound to lbvserver.
lbvserver_analyticsprofile_binding	<lbvserver_analyticsprofile_binding[]>	Read-only	analyticsprofile that can be bound to lbvserver.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_binding/ name_value<String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "lbvserver_binding": [ {

"name":<String_value>,

"lbvserver_videooptimizationdetectionpolicy_binding":<lbvserver_videooptim
izationdetectionpolicy_binding[]_value>,

"lbvserver_botpolicy_binding":<lbvserver_botpolicy_binding[]_value>,

"lbvserver_auditnslogpolicy_binding":<lbvserver_auditnslogpolicy_binding[]
_value>,

"lbvserver_appqoepolicy_binding":<lbvserver_appqoepolicy_binding[]_value>,

"lbvserver_authorizationpolicy_binding":<lbvserver_authorizationpolicy_bin
ding[]_value>,

"lbvserver_feopolicy_binding":<lbvserver_feopolicy_binding[]_value>,

"lbvserver_cmppolicy_binding":<lbvserver_cmppolicy_binding[]_value>,

"lbvserver_appflowpolicy_binding":<lbvserver_appflowpolicy_binding[]_value
>,

"lbvserver_appfwpolicy_binding":<lbvserver_appfwpolicy_binding[]_value>,

"lbvserver_cachepolicy_binding":<lbvserver_cachepolicy_binding[]_value>,

"lbvserver_servicegroupmember_binding":<lbvserver_servicegroupmember_bindi
ng[]_value>,

"lbvserver_analyticsprofile_binding":<lbvserver_analyticsprofile_binding[]
_value>,
```

```
"lbvserver_csvserver_binding":<lbvserver_csvserver_binding[]_value>,

"lbvserver_rewritepolicy_binding":<lbvserver_rewritepolicy_binding[]_value
>,

"lbvserver_spilloverpolicy_binding":<lbvserver_spilloverpolicy_binding[]_v
alue>,

"lbvserver_videooptimizationpacingpolicy_binding":<lbvserver_videooptimiza
tionpacingpolicy_binding[]_value>,

"lbvserver_transformpolicy_binding":<lbvserver_transformpolicy_binding[]_v
alue>,

"lbvserver_lbpolicy_binding":<lbvserver_lbpolicy_binding[]_value>,

"lbvserver_responderpolicy_binding":<lbvserver_responderpolicy_binding[]_v
alue>,

"lbvserver_service_binding":<lbvserver_service_binding[]_value>,

"lbvserver_servicegroup_binding":<lbvserver_servicegroup_binding[]_value>,

"lbvserver_contentinspectionpolicy_binding":<lbvserver_contentinspectionpo
licy_binding[]_value>,

"lbvserver_tmtrafficpolicy_binding":<lbvserver_tmtrafficpolicy_binding[]_v
alue>,

"lbvserver_dnspolicy64_binding":<lbvserver_dnspolicy64_binding[]_value>,

"lbvserver_auditsyslogpolicy_binding":<lbvserver_auditsyslogpolicy_binding
[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "lbvserver_binding": [ {

"name":<String_value>,

"lbvserver_videooptimizationdetectionpolicy_binding":<lbvserver_videooptim
izationdetectionpolicy_binding[]_value>,

"lbvserver_botpolicy_binding":<lbvserver_botpolicy_binding[]_value>,

"lbvserver_auditnslogpolicy_binding":<lbvserver_auditnslogpolicy_binding[]
_value>,

"lbvserver_appqoepolicy_binding":<lbvserver_appqoepolicy_binding[]_value>,

"lbvserver_authorizationpolicy_binding":<lbvserver_authorizationpolicy_bin
ding[]_value>,

"lbvserver_feopolicy_binding":<lbvserver_feopolicy_binding[]_value>,

"lbvserver_cmppolicy_binding":<lbvserver_cmppolicy_binding[]_value>,

"lbvserver_appflowpolicy_binding":<lbvserver_appflowpolicy_binding[]_value
```

```
>,

"lbvserver_appfwpolicy_binding":<lbvserver_appfwpolicy_binding[]_value>,

"lbvserver_cachepolicy_binding":<lbvserver_cachepolicy_binding[]_value>,

"lbvserver_servicegroupmember_binding":<lbvserver_servicegroupmember_bindi
ng[]_value>,

"lbvserver_analyticsprofile_binding":<lbvserver_analyticsprofile_binding[]
_value>,

"lbvserver_csvserver_binding":<lbvserver_csvserver_binding[]_value>,

"lbvserver_rewritepolicy_binding":<lbvserver_rewritepolicy_binding[]_value
>,

"lbvserver_spilloverpolicy_binding":<lbvserver_spilloverpolicy_binding[]_v
alue>,

"lbvserver_videooptimizationpacingpolicy_binding":<lbvserver_videooptimiza
tionpacingpolicy_binding[]_value>,

"lbvserver_transformpolicy_binding":<lbvserver_transformpolicy_binding[]_v
alue>,

"lbvserver_lbpolicy_binding":<lbvserver_lbpolicy_binding[]_value>,

"lbvserver_responderpolicy_binding":<lbvserver_responderpolicy_binding[]_v
alue>,

"lbvserver_service_binding":<lbvserver_service_binding[]_value>,

"lbvserver_servicegroup_binding":<lbvserver_servicegroup_binding[]_value>,

"lbvserver_contentinspectionpolicy_binding":<lbvserver_contentinspectionpo
licy_binding[]_value>,

"lbvserver_tmtrafficpolicy_binding":<lbvserver_tmtrafficpolicy_binding[]_v
alue>,

"lbvserver_dnspolicy64_binding":<lbvserver_dnspolicy64_binding[]_value>,

"lbvserver_auditsyslogpolicy_binding":<lbvserver_auditsyslogpolicy_binding
```

```
[]_value>

}]}
```

lbvserver_botpolicy_binding

Binding object showing the botpolicy that can be bound to lbvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the virtual server. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at sign (@), equal sign (=), and hyphen (-) characters. Can be changed after the virtual server is created.

CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my vserver" or 'my vserver'). .

Minimum length = 1

Possible values = reqvserver, resvserver, policylabel

Possible values = REQUEST, RESPONSE, MQTT_JUMBO_REQ

Minimum value = 1

Maximum value = 8192

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/lbvserver_botpolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"lbvserver_botpolicy_binding":{

<b>"name":<String_value>,

</b>"policyname":<String_value>,

"priority":<Integer_value>,

"gotopriorityexpression":<String_value>,

"bindpoint":<String_value>,

"invoke":<Boolean_value>,

"labeltype":<String_value>,

"labelname":<String_value>,

"order":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_botpolicy_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/

lbvserver_botpolicy_binding/ name_value<String> ? **args=policyname: <String_value> ,bindpoint: <String_value> ,priority: <Integer_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_botpolicy_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ lbvserver_botpolicy_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of lbvserver_botpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_botpolicy_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the lbvserver_botpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lbvserver_botpolicy_binding": [ {

"name":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"bindpoint":<String_value>,

"order":<Integer_value>,

"labelname":<String_value>,

"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>,

"policyname":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_botpolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_botpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lbvserver_botpolicy_binding": [ {

"name":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"bindpoint":<String_value>,

"order":<Integer_value>,

"labelname":<String_value>,

"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>,

"policyname":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_botpolicy_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"lbvserver_botpolicy_binding": [ { "__count": "#no"} ] }
```

lbvserver_cachepolicy_binding

Binding object showing the cachepolicy that can be bound to lbvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
order	<Integer>	Read-write	Integer specifying the order of the service. A larger number specifies a lower order. Defines the order of the service relative to the other services in the load balancing vserver's bindings. Determines the priority given to the service among all the services bound. Minimum value = 1 Maximum value = 8192
labelname	<String>	Read-write	Name of the label invoked.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
labeltype	<String>	Read-write	The invocation type. Possible values = reqvserver, resvserver, policylabel
priority	<Integer>	Read-write	Priority.
bindpoint	<String>	Read-write	The bindpoint to which the policy is bound. Possible values = REQUEST, RESPONSE, MQTT_JUMBO_REQ
name	<String>	Read-write	Name for the virtual server. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at sign (@), equal sign (=), and hyphen (-) characters. Can be changed after the virtual server is created.

CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my vserver" or 'my vserver'). .

Minimum length = 1

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/lbvserver_cachepolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"lbvserver_cachepolicy_binding":{

<b>"name":<String_value>,

</b>"policyname":<String_value>,

"priority":<Integer_value>,

"gotopriorityexpression":<String_value>,

"bindpoint":<String_value>,

"invoke":<Boolean_value>,

"labeltype":<String_value>,

"labelname":<String_value>,

"order":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_cachepolicy_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ lbvserver_cachepolicy_binding/ name_value<String> ? **args=policyname: <String_value> ,bindpoint: <String_value> ,priority: <Integer_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_cachepolicy_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ lbvserver_cachepolicy_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of lbvserver_cachepolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_cachepolicy_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the lbvserver_cachepolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lbvserver_cachepolicy_binding": [ {

"order":<Integer_value>,

"labelname":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"bindpoint":<String_value>,

"name":<String_value>,

"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>,

"policyname":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_cachepolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_cachepolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lbvserver_cachepolicy_binding": [ {

"order":<Integer_value>,

"labelname":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"bindpoint":<String_value>,

"name":<String_value>,

"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>,

"policyname":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_cachepolicy_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"lbvserver_cachepolicy_binding": [ { "__count": "#no"} ] }
```

lbvserver_cmppolicy_binding

Binding object showing the cmppolicy that can be bound to lbvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
labelname	<String>	Read-write	Name of the label invoked.
order	<Integer>	Read-write	Integer specifying the order of the service. A larger number specifies a lower order. Defines the order of the service relative to the other services in the load balancing vserver's bindings. Determines the priority given to the service among all the services bound. Minimum value = 1 Maximum value = 8192

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the virtual server. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at sign (@), equal sign (=), and hyphen (-) characters. Can be changed after the virtual server is created.

CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my vserver" or 'my vserver'). .

Minimum length = 1

Possible values = reqvserver, resvserver, policylabel

Possible values = REQUEST, RESPONSE, MQTT_JUMBO_REQ

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/lbvserver_cmppolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"lbvserver_cmppolicy_binding":{

<b>"name":<String_value>,
```

```
</b>"policyname":<String_value>,

"priority":<Integer_value>,

"gotopriorityexpression":<String_value>,

"bindpoint":<String_value>,

"invoke":<Boolean_value>,

"labeltype":<String_value>,

"labelname":<String_value>,

"order":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_cmppolicy_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ lbvserver_cmppolicy_binding/ name_value<String> ? **args=policyname: <String_value> ,bindpoint: <String_value> ,priority: <Integer_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_cmppolicy_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ lbvserver_cmppolicy_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of lbvserver_cmppolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_cmppolicy_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the lbvserver_cmppolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lbvserver_cmppolicy_binding": [ {

"labelname":<String_value>,

"order":<Integer_value>,

"name":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,
```

```
"bindpoint":<String_value>,

"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>,

"policyname":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_cmppolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_cmppolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lbvserver_cmppolicy_binding": [ {

"labelname":<String_value>,
```

```
"order":<Integer_value>,

"name":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"bindpoint":<String_value>,

"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>,

"policyname":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_cmppolicy_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"lbvserver_cmppolicy_binding": [ { "__count": "#no"} ] }
```

lbvserver_contentinspectionpolicy_binding

Binding object showing the contentinspectionpolicy that can be bound to lbvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
policyname	<String>	Read-write	Name of the policy bound to the LB vserver.
gotopriorityexpression	<String>	Read-write	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
invoke	<Boolean>	Read-write	Invoke policies bound to a virtual server or policy label.
labeltype	<String>	Read-write	The invocation type. Possible values = reqvserver, resvserver, policylabel
priority	<Integer>	Read-write	Priority.
bindpoint	<String>	Read-write	The bindpoint to which the policy is bound. Possible values = REQUEST, RESPONSE, MQTT_JUMBO_REQ

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the virtual server. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at sign (@), equal sign (=), and hyphen (-) characters. Can be changed after the virtual server is created.

CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my vserver" or 'my vserver'). .

Minimum length = 1

Minimum value = 1

Maximum value = 8192

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/lbvserver_contentinspectionpolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"lbvserver_contentinspectionpolicy_binding":{

<b>"name":<String_value>,
```

```
</b>"policyname":<String_value>,

"priority":<Integer_value>,

"gotopriorityexpression":<String_value>,

"bindpoint":<String_value>,

"invoke":<Boolean_value>,

"labeltype":<String_value>,

"labelname":<String_value>,

"order":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_contentinspectionpolicy_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ lbvserver_contentinspectionpolicy_binding/ name_value<String> ? **args=policyname: <String_value> ,bindpoint: <String_value> ,priority: <Integer_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_contentinspectionpolicy_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ lbvserver_contentinspectionpolicy_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of lbvserver_contentinspectionpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ lbvserver_contentinspectionpolicy_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the lbvserver_contentinspectionpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lbvserver_contentinspectionpolicy_binding": [ {

"policyname":<String_value>,

"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>,

"labeltype":<String_value>,
```

```
"priority":<Integer_value>,

"bindpoint":<String_value>,

"name":<String_value>,

"order":<Integer_value>,

"labelname":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_contentinspectionpolicy_binding
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_contentinspectionpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lbvserver_contentinspectionpolicy_binding": [ {

"policyname":<String_value>,

"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"bindpoint":<String_value>,

"name":<String_value>,

"order":<Integer_value>,

"labelname":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_contentinspectionpolicy_binding/name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"lbvserver_contentinspectionpolicy_binding": [ { "__count": "#no"} ] }
```

lbvserver_csvserver_binding

Binding object showing the csvserver that can be bound to lbvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
order	<Integer>	Read-write	Integer specifying the order of the service. A larger number specifies a lower order. Defines the order of the service relative to the other services in the load balancing vserver's bindings. Determines the priority given to the service among all the services bound. Minimum value = 1 Maximum value = 8192
priority	<Integer>	Read-write	Priority.
cachevserver	<String>	Read-write	Cache virtual server.
name	<String>	Read-write	Name for the virtual server. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			alphanumeric, underscore, hash (#), period (.), space, colon (:), at sign (@), equal sign (=), and hyphen (-) characters. Can be changed after the virtual server is created.

CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my vserver" or 'my vserver'). .

Minimum length = 1

Possible values = TRANSPARENT, REVERSE, FORWARD

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_csvserver_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ lbvserver_csvserver_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of lbvserver_csvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_csvserver_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the lbvserver_csvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lbvserver_csvserver_binding": [ {

"order":<Integer_value>,

"priority":<Integer_value>,

"cachevserver":<String_value>,

"name":<String_value>,

"policyname":<String_value>,

"pipolicyhits":<Integer_value>,

"cachetype":<String_value>,

"policysubtype":<Integer_value>,

"hits":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_csvserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_csvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lbvserver_csvserver_binding": [ {

"order":<Integer_value>,

"priority":<Integer_value>,

"cachevserver":<String_value>,

"name":<String_value>,

"policyname":<String_value>,

"pipolicyhits":<Integer_value>,

"cachetype":<String_value>,

"policysubtype":<Integer_value>,

"hits":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_csvserver_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"lbvserver_csvserver_binding": [ { "__count": "#no"} ] }
```

lbvserver_dnspolicy64_binding

Binding object showing the dnspolicy64 that can be bound to lbvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
policyname	<String>	Read-write	Name of the policy bound to the LB vserver.
gotopriorityexpression	<String>	Read-write	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
invoke	<Boolean>	Read-write	Invoke policies bound to a virtual server or policy label.
labelname	<String>	Read-write	Name of the virtual server or user-defined policy label to invoke if the policy evaluates to TRUE.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
order	<Integer>	Read-write	Integer specifying the order of the service. A larger number specifies a lower order. Defines the order of the service relative to the other services in the load balancing vserver's bindings. Determines the priority given to the service among all the services bound. Minimum value = 1 Maximum value = 8192
name	<String>	Read-write	Name for the virtual server. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at sign (@), equal sign (=), and hyphen (-) characters. Can be changed after the virtual server is created.

CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my vserver" or 'my vserver'). .

Minimum length = 1

Possible values = REQUEST, RESPONSE, MQTT_JUMBO_REQ

Possible values = reqvserver, resvserver, policylabel

```
</td></tr><tr><td>priority

</td><td>&lt;Integer&gt;

</td><td>Read-write

</td><td>Priority.

</td></tr><tr><td>__count

</td><td>&lt;Double&gt;

</td><td>Read-write

</td><td>count parameter

</td></tr></tbody></table>
```

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/lbvserver_dnspolicy64_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"lbvserver_dnspolicy64_binding":{

<b>"name":<String_value>,

</b>"policyname":<String_value>,

"priority":<Integer_value>,

"gotopriorityexpression":<String_value>,
```

```
"bindpoint":<String_value>,

"invoke":<Boolean_value>,

"labeltype":<String_value>,

"labelname":<String_value>,

"order":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_dnspolicy64_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ lbvserver_dnspolicy64_binding/ name_value<String> ? **args=policyname: <String_value> ,bindpoint: <String_value> ,priority: <Integer_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_dnspolicy64_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ lbvserver_dnspolicy64_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of lbvserver_dnspolicy64_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_dnspolicy64_binding/name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the lbvserver_dnspolicy64_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lbvserver_dnspolicy64_binding": [ {

"policyname":<String_value>,

"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>,

"labelname":<String_value>,

"order":<Integer_value>,

"name":<String_value>,

"bindpoint":<String_value>,

"labeltype":<String_value>,
```

```
"priority":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_dnspolicy64_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_dnspolicy64_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lbvserver_dnspolicy64_binding": [ {

"policyname":<String_value>,

"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>,

"labelname":<String_value>,
```

```
"order":<Integer_value>,

"name":<String_value>,

"bindpoint":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_dnspolicy64_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"lbvserver_dnspolicy64_binding": [ { "__count": "#no"} ] }
```

lbvserver_feopolicy_binding

Binding object showing the feopolicy that can be bound to lbvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
labelname	<String>	Read-write	Name of the virtual server or user-defined policy label to invoke if the policy evaluates to TRUE.
order	<Integer>	Read-write	Integer specifying the order of the service. A larger number specifies a lower order. Defines the order of the service relative to the other services in the load balancing vserver's bindings. Determines the priority given to the service among all the services bound. Minimum value = 1 Maximum value = 8192
bindpoint	<String>	Read-write	The bindpoint to which the policy is bound. Possible values = REQUEST, RESPONSE, MQTT_JUMBO_REQ
priority	<Integer>	Read-write	Priority.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
labeltype	<String>	Read-write	Type of policy label to invoke. Applicable only to rewrite, videooptimization and cache policies. Available settings function as follows: * reqvserver - Evaluate the request against the request-based policies bound to the specified virtual server. * resvserver - Evaluate the response against the response-based policies bound to the specified virtual server. * policylabel - invoke the request or response against the specified user-defined policy label. Possible values = reqvserver, resvserver, policylabel
name	<String>	Read-write	Name for the virtual server. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at sign (@), equal sign (=), and

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			hyphen (-) characters. Can be changed after the virtual server is created.

CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my vserver" or 'my vserver'). .

Minimum length = 1

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/lbvserver_feopolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"lbvserver_feopolicy_binding":{

<b>"name":<String_value>,

</b>"policyname":<String_value>,

"priority":<Integer_value>,

"gotopriorityexpression":<String_value>,

"bindpoint":<String_value>,

"invoke":<Boolean_value>,

"labeltype":<String_value>,

"labelname":<String_value>,

"order":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_feopolicy_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ lbvserver_feopolicy_binding/ name_value<String> ? **args=policyname: <String_value> ,bindpoint: <String_value> ,priority: <Integer_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_feopolicy_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ lbvserver_feopolicy_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of lbvserver_feopolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_feopolicy_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the lbvserver_feopolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lbvserver_feopolicy_binding": [ {

"labelname":<String_value>,

"order":<Integer_value>,

"bindpoint":<String_value>,

"priority":<Integer_value>,

"labeltype":<String_value>,

"name":<String_value>,

"invoke":<Boolean_value>,

"gotopriorityexpression":<String_value>,

"policyname":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_feopolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_feopolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lbvserver_feopolicy_binding": [ {

"labelname":<String_value>,

"order":<Integer_value>,

"bindpoint":<String_value>,

"priority":<Integer_value>,

"labeltype":<String_value>,

"name":<String_value>,

"invoke":<Boolean_value>,

"gotopriorityexpression":<String_value>,

"policyname":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_feopolicy_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"lbvserver_feopolicy_binding": [ { "__count": "#no"} ] }
```

lbvserver_lbpolicy_binding

Binding object showing the lbpolicy that can be bound to lbvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
labelname	<String>	Read-write	Name of the label invoked.
order	<Integer>	Read-write	Integer specifying the order of the service. A larger number specifies a lower order. Defines the order of the service relative to the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			other services in the load balancing vserver's bindings. Determines the priority given to the service among all the services bound. Minimum value = 1 Maximum value = 8192
priority	<Integer>	Read-write	Priority.
labeltype	<String>	Read-write	The invocation type. Possible values = reqvserver, resvserver, policylabel
bindpoint	<String>	Read-write	The bindpoint to which the policy is bound. Possible values = REQUEST, RESPONSE, MQTT_JUMBO_REQ
name	<String>	Read-write	Name for the virtual server. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at sign (@),

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			equal sign (=), and hyphen (-) characters. Can be changed after the virtual server is created.

CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my vserver" or 'my vserver'). .

Minimum length = 1

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/lbvserver_lbpolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"lbvserver_lbpolicy_binding":{

<b>"name":<String_value>,

</b>"policyname":<String_value>,

"priority":<Integer_value>,

"gotopriorityexpression":<String_value>,

"bindpoint":<String_value>,

"invoke":<Boolean_value>,

"labeltype":<String_value>,

"labelname":<String_value>,

"order":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_lbpolicy_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ lbvserver_lbpolicy_binding/ name_value<String> ? **args=policyname: <String_value> ,bindpoint: <String_value> ,priority: <Integer_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_lbpolicy_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ lbvserver_lbpolicy_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of lbvserver_lbpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_lbpolicy_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the lbvserver_lbpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lbvserver_lbpolicy_binding": [ {

"labelname":<String_value>,

"order":<Integer_value>,

"priority":<Integer_value>,

"labeltype":<String_value>,

"bindpoint":<String_value>,

"name":<String_value>,

"policyname":<String_value>,

"invoke":<Boolean_value>,

"gotopriorityexpression":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_lbpolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_lbpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lbvserver_lbpolicy_binding": [ {

"labelname":<String_value>,

"order":<Integer_value>,

"priority":<Integer_value>,

"labeltype":<String_value>,

"bindpoint":<String_value>,

"name":<String_value>,

"policyname":<String_value>,

"invoke":<Boolean_value>,

"gotopriorityexpression":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_lbpolicy_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"lbvserver_lbpolicy_binding": [ { "__count": "#no"} ] }
```

lbvserver_responderpolicy_binding

Binding object showing the responderpolicy that can be bound to lbvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
gotopriorityexpression	<String>	Read-write	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
invoke	<Boolean>	Read-write	Invoke policies bound to a virtual server or policy label.
policyname	<String>	Read-write	Name of the policy bound to the LB vserver.
labeltype	<String>	Read-write	The invocation type. Possible values = reqvserver, resvserver, policylabel
priority	<Integer>	Read-write	Priority.
bindpoint	<String>	Read-write	The bindpoint to which the policy is bound. Possible values = REQUEST, RESPONSE, MQTT_JUMBO_REQ
name	<String>	Read-write	Name for the virtual server. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at sign (@), equal sign (=), and hyphen (-) characters. Can be changed after the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			virtual server is created.

CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my vserver" or 'my vserver'). .

Minimum length = 1

Minimum value = 1

Maximum value = 8192

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/lbvserver_responderpolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"lbvserver_responderpolicy_binding":{

<b>"name":<String_value>,

</b>"policyname":<String_value>,

"priority":<Integer_value>,

"gotopriorityexpression":<String_value>,

"bindpoint":<String_value>,

"invoke":<Boolean_value>,

"labeltype":<String_value>,

"labelname":<String_value>,

"order":<Integer_value>
```

```
}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_responderpolicy_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ lbvserver_responderpolicy_binding/ name_value<String> ? **args=policyname: <String_value> ,bindpoint: <String_value> ,priority: <Integer_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_responderpolicy_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ lbvserver_responderpolicy_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of lbvserver_responderpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_responderpolicy_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the lbvserver_responderpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lbvserver_responderpolicy_binding": [ {

"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>,

"policyname":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"bindpoint":<String_value>,

"name":<String_value>,

"labelname":<String_value>,

"order":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_responderpolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_responderpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lbvserver_responderpolicy_binding": [ {

"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>,

"policyname":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"bindpoint":<String_value>,

"name":<String_value>,

"labelname":<String_value>,

"order":<Integer_value>

}]}
```

```
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_responderpolicy_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"lbvserver_responderpolicy_binding": [ { "__count": "#no"} ] }
```

lbvserver_rewritepolicy_binding

Binding object showing the rewritepolicy that can be bound to lbvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the virtual server. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			underscore, hash (#), period (.), space, colon (:), at sign (@), equal sign (=), and hyphen (-) characters. Can be changed after the virtual server is created.

CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my vserver" or 'my vserver'). .

Minimum length = 1

Possible values = REQUEST, RESPONSE, MQTT_JUMBO_REQ

Possible values = reqvserver, resvserver, policylabel

Minimum value = 1

Maximum value = 8192

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/lbvserver_rewritepolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"lbvserver_rewritepolicy_binding":{

<b>"name":<String_value>,

</b>"policyname":<String_value>,

"priority":<Integer_value>,

"gotopriorityexpression":<String_value>,
```

```
"bindpoint":<String_value>,

"invoke":<Boolean_value>,

"labeltype":<String_value>,

"labelname":<String_value>,

"order":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_rewritepolicy_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ lbvserver_rewritepolicy_binding/ name_value<String> ? **args=policyname: <String_value> ,bindpoint: <String_value> ,priority: <Integer_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_rewritepolicy_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ lbvserver_rewritepolicy_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of lbvserver_rewritepolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_rewritepolicy_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the lbvserver_rewritepolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lbvserver_rewritepolicy_binding": [ {

"name":<String_value>,

"bindpoint":<String_value>,

"priority":<Integer_value>,

"labeltype":<String_value>,

"order":<Integer_value>,

"labelname":<String_value>,

"invoke":<Boolean_value>,

"gotopriorityexpression":<String_value>,
```

```
"policyname":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_rewritepolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_rewritepolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lbvserver_rewritepolicy_binding": [ {

"name":<String_value>,

"bindpoint":<String_value>,

"priority":<Integer_value>,

"labeltype":<String_value>,
```

```
"order":<Integer_value>,

"labelname":<String_value>,

"invoke":<Boolean_value>,

"gotopriorityexpression":<String_value>,

"policyname":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_rewritepolicy_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"lbvserver_rewritepolicy_binding": [ { "__count": "#no"} ] }
```

lbvserver_service_binding

Binding object showing the service that can be bound to lbvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
weight	<Integer>	Read-write	Weight to assign to the specified service. Minimum value = 1 Maximum value = 100
servicegroupname	<String>	Read-write	Name of the service group. Minimum length = 1
name	<String>	Read-write	Name for the virtual server. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at sign (@), equal sign (=), and hyphen (-) characters. Can be changed after the virtual server is created.

CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my vserver" or 'my vserver'). .

Minimum length = 1

Minimum value = 1

Maximum value = 8192

Minimum length = 1

Possible values = UP, DOWN, UNKNOWN, BUSY, OUT OF SERVICE, GOING OUT OF SERVICE, DOWN WHEN GOING OUT OF SERVICE, NS_EMPTY_STR, Unknown, DISABLED

Range 1 - 65535

* in CLI is represented as 65535 in NITRO API

Possible values = HTTP, FTP, TCP, UDP, SSL, SSL_BRIDGE, SSL_TCP, DTLS, NNTP, DNS, DHCPRA, ANY, SIP_UDP, SIP_TCP, SIP_SSL, DNS_TCP, RTSP, PUSH, SSL_PUSH, RADIUS, RDP, MYSQL, MSSQL, DIAMETER, SSL_DIAMETER, TFTP, ORACLE, SMPP, SYSLOGTCP, SYSLOGUDP, FIX, SSL_FIX, PROXY, USER_TCP, USER_SSL_TCP, QUIC, IPFIX, LOGSTREAM, MONGO, MONGO_TLS, MQTT, MQTT_TLS, QUIC_BRIDGE, HTTP_QUIC, DOT, SSL_PROXY, KAFKA_PRODUCER

Range 1 - 65535

* in CLI is represented as 65535 in NITRO API

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/lbvserver_service_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"lbvserver_service_binding":{

<b>"name":<String_value>,

</b>"servicename":<String_value>,

"weight":<Integer_value>,

"servicegroupname":<String_value>,

"order":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_service_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ lbvserver_service_binding/ name_value<String> ? **args=servicename: <String_value> ,servicegroupname: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_service_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ lbvserver_service_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of lbvserver_service_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_service_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the lbvserver_service_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lbvserver_service_binding": [ {

"weight":<Integer_value>,

"servicegroupname":<String_value>,

"name":<String_value>,

"order":<Integer_value>,

"servicename":<String_value>,

"vserverid":<String_value>,

"curstate":<String_value>,

"port":<Integer_value>,

"servicetype":<String_value>,

"preferredlocation":<String_value>,

"ipv46":<String_value>,

"vsvrbindsvcip":<String_value>,

"dynamicweight":<Integer_value>,

"cookieipport":<String_value>,

"vsvrbindsvcport":<Integer_value>,
```

```
"cookiename":<String_value>,

"orderstr":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_service_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_service_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lbvserver_service_binding": [ {

"weight":<Integer_value>,

"servicegroupname":<String_value>,

"name":<String_value>,

"order":<Integer_value>,
```

```
"servicename":<String_value>,

"vserverid":<String_value>,

"curstate":<String_value>,

"port":<Integer_value>,

"servicetype":<String_value>,

"preferredlocation":<String_value>,

"ipv46":<String_value>,

"vsvrbindsvcip":<String_value>,

"dynamicweight":<Integer_value>,

"cookieipport":<String_value>,

"vsvrbindsvcport":<Integer_value>,

"cookiename":<String_value>,

"orderstr":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_service_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"lbvserver_service_binding": [ { "__count": "#no"} ] }
```

lbvserver_servicegroup_binding

Binding object showing the servicegroup that can be bound to lbvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
weight	<Integer>	Read-write	Integer specifying the weight of the service. A larger number specifies a greater weight. Defines the capacity of the service relative to the other services in the load balancing configuration. Determines the priority given to the service in load balancing decisions. Default value: 1 Minimum value = 1 Maximum value = 100

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
servicegroupname	<String>	Read-write	The service group name bound to the selected load balancing virtual server.
name	<String>	Read-write	Name for the virtual server. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at sign (@), equal sign (=), and hyphen (-) characters. Can be changed after the virtual server is created.

CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my vserver" or 'my vserver'). .

Minimum length = 1

Minimum value = 1

Maximum value = 8192

Minimum length = 1

Operations

(click to see Properties)

- ADD
- DELETE

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/lbvserver_servicegroup_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"lbvserver_servicegroup_binding":{

<b>"name":<String_value>,

</b>"servicename":<String_value>,

"weight":<Integer_value>,

"servicegroupname":<String_value>,

"order":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_servicegroup_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ lbvserver_servicegroup_binding/ name_value<String> ? **args=servicename: <String_value> ,servicegroupname: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_servicegroup_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/

lbvserver_servicegroup_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of lbvserver_servicegroup_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_servicegroup_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the lbvserver_servicegroup_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lbvserver_servicegroup_binding": [ {

"weight":<Integer_value>,

"servicegroupname":<String_value>,

"name":<String_value>,

"order":<Integer_value>,

"servicename":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_servicegroup_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_servicegroup_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lbvserver_servicegroup_binding": [ {

"weight":<Integer_value>,

"servicegroupname":<String_value>,

"name":<String_value>,

"order":<Integer_value>,

"servicename":<String_value>

}]}
```

```
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_servicegroup_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"lbvserver_servicegroup_binding": [ { "__count": "#no"} ] }
```

lbvserver_servicegroupmember_binding

Binding object showing the servicegroupmember that can be bound to lbvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
order	<Integer>	Read-write	Order number to be assigned to the service when it is bound to the lb vserver. Minimum value = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum value = 8192
servicegroupname	<String>	Read-write	The service group name bound to the selected load balancing virtual server.
name	<String>	Read-write	Name for the virtual server. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at sign (@), equal sign (=), and hyphen (-) characters. Can be changed after the virtual server is created.

CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my vserver" or 'my vserver'). .

Minimum length = 1

Minimum value = 1

Maximum value = 100

Possible values = HTTP, FTP, TCP, UDP, SSL, SSL_BRIDGE, SSL_TCP, DTLS, NNTP, DNS, DHCPRA, ANY, SIP_UDP, SIP_TCP, SIP_SSL, DNS_TCP, RTSP, PUSH, SSL_PUSH, RADIUS, RDP, MYSQL, MSSQL, DIAMETER, SSL_DIAMETER, TFTP, ORACLE, SMPP, SYSLOGTCP, SYSLOGUDP, FIX, SSL_FIX, PROXY, USER_TCP, USER_SSL_TCP, QUIC, IPFIX,

LOGSTREAM, MONGO, MONGO_TLS, MQTT, MQTT_TLS, QUIC_BRIDGE, HTTP_QUIC, DOT, SSL_PROXY, KAFKA_PRODUCER

Range 1 - 65535

* in CLI is represented as 65535 in NITRO API

Possible values = UP, DOWN, UNKNOWN, BUSY, OUT OF SERVICE, GOING OUT OF SERVICE, DOWN WHEN GOING OUT OF SERVICE, NS_EMPTY_STR, Unknown, DISABLED

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_servicegroupmember_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ lbvserver_servicegroupmember_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of lbvserver_servicegroupmember_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_servicegroupmember_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the lbvserver_servicegroupmember_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lbvserver_servicegroupmember_binding": [ {

"order":<Integer_value>,

"servicegroupname":<String_value>,

"name":<String_value>,

"weight":<Integer_value>,
```

```
"servicetype":<String_value>,

"port":<Integer_value>,

"vserverid":<String_value>,

"curstate":<String_value>,

"ipv46":<String_value>,

"preferredlocation":<String_value>,

"cookiename":<String_value>,

"orderstr":<String_value>,

"cookieipport":<String_value>,

"dynamicweight":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_servicegroupmember_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_servicegroupmember_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lbvserver_servicegroupmember_binding": [ {

"order":<Integer_value>,

"servicegroupname":<String_value>,

"name":<String_value>,

"weight":<Integer_value>,

"servicetype":<String_value>,

"port":<Integer_value>,

"vserverid":<String_value>,

"curstate":<String_value>,

"ipv46":<String_value>,

"preferredlocation":<String_value>,

"cookiename":<String_value>,

"orderstr":<String_value>,

"cookieipport":<String_value>,

"dynamicweight":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_servicegroupmember_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"lbvserver_servicegroupmember_binding": [ { "__count": "#no"} ] }
```

lbvserver_spilloverpolicy_binding

Binding object showing the spilloverpolicy that can be bound to lbvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the virtual server. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			colon (:), at sign (@), equal sign (=), and hyphen (-) characters. Can be changed after the virtual server is created.

CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my vserver" or 'my vserver'). .

Minimum length = 1

Possible values = REQUEST, RESPONSE, MQTT_JUMBO_REQ

Possible values = reqvserver, resvserver, policylabel

```
 </td></tr><tr><td>priority

 </td><td>&lt;Integer&gt;

 </td><td>Read-write

 </td><td>Priority.

 </td></tr><tr><td>order

 </td><td>&lt;Integer&gt;

 </td><td>Read-write

 </td><td>Integer specifying the order of the service. A larger number
specifies a lower order. Defines the order of the service relative to the
other services in the load balancing vserver's bindings. Determines the
priority given to the service among all the services bound.

  <p>Minimum value =  1</p>

  <p>Maximum value =  8192</p>

 </td></tr><tr><td>labelname
```

```
</td><td>&lt;String&gt;

</td><td>Read-write

</td><td>Name of the virtual server or user-defined policy label to
invoke if the policy evaluates to TRUE.

</td></tr><tr><td>policyname

</td><td>&lt;String&gt;

</td><td>Read-write

</td><td>Name of the policy bound to the LB vserver.

</td></tr><tr><td>gotopriorityexpression

</td><td>&lt;String&gt;

</td><td>Read-write

</td><td>Expression specifying the priority of the next policy which will
get evaluated if the current policy rule evaluates to TRUE.

</td></tr><tr><td>invoke

</td><td>&lt;Boolean&gt;

</td><td>Read-write

</td><td>Invoke policies bound to a virtual server or policy label.

</td></tr><tr><td>__count

</td><td>&lt;Double&gt;

</td><td>Read-write

</td><td>count parameter

</td></tr></tbody></table>
```

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/lbvserver_spilloverpolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"lbvserver_spilloverpolicy_binding":{

<b>"name":<String_value>,

</b>"policyname":<String_value>,

"priority":<Integer_value>,

"gotopriorityexpression":<String_value>,

"bindpoint":<String_value>,

"invoke":<Boolean_value>,

"labeltype":<String_value>,

"labelname":<String_value>,

"order":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_spilloverpolicy_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ lbvserver_spilloverpolicy_binding/ name_value<String> ? **args=policyname: <String_value> ,bindpoint: <String_value> ,priority: <Integer_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_spilloverpolicy_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ lbvserver_spilloverpolicy_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of lbvserver_spilloverpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_spilloverpolicy_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the lbvserver_spilloverpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lbvserver_spilloverpolicy_binding": [ {

"name":<String_value>,

"bindpoint":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"order":<Integer_value>,

"labelname":<String_value>,

"policyname":<String_value>,

"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_spilloverpolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_spilloverpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lbvserver_spilloverpolicy_binding": [ {

"name":<String_value>,

"bindpoint":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"order":<Integer_value>,

"labelname":<String_value>,

"policyname":<String_value>,

"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_spilloverpolicy_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"lbvserver_spilloverpolicy_binding": [ { "__count": "#no"} ] }
```

lbvserver_tmtrafficpolicy_binding

Binding object showing the tmtrafficpolicy that can be bound to lbvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
policyname	<String>	Read-write	Name of the policy bound to the LB vserver.
gotopriorityexpression	<String>	Read-write	Expression or other value specifying the next policy to be evaluated if the current policy evaluates to TRUE. Specify one of the following values: * NEXT - Evaluate the policy with the next higher priority number. * END - End policy evaluation. * USE_INVOCATION_RESULT - Applicable if this policy invokes another policy label. If the final goto in the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			invoked policy label has a value of END, the evaluation stops. If the final goto is anything other than END, the current policy label performs a NEXT. * An expression that evaluates to a number. If you specify an expression, the number to which it evaluates determines the next policy to evaluate, as follows: * If the expression evaluates to a higher numbered priority, the policy with that priority is evaluated next. * If the expression evaluates to the priority of the current policy, the policy with the next higher numbered priority is evaluated next. * If the expression evaluates to a priority number that is numerically higher than the highest numbered priority, policy evaluation ends. An UNDEF event is triggered if: * The expression is invalid.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			* The expression evaluates to a priority number that is numerically lower than the current policy's priority. * The expression evaluates to a priority number that is between the current policy's priority number (say, 30) and the highest priority number (say, 100), but does not match any configured priority number (for example, the expression evaluates to the number 85). This example assumes that the priority number increments by 10 for every successive policy, and therefore a priority number of 85 does not exist in the policy label.
invoke	<Boolean>	Read-write	Invoke policies bound to a virtual server or policy label.
order	<Integer>	Read-write	Integer specifying the order of the service. A larger number specifies a lower order. Defines the order of the service relative to the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			other services in the load balancing vserver's bindings. Determines the priority given to the service among all the services bound. Minimum value = 1 Maximum value = 8192
labelname	<String>	Read-write	Name of the virtual server or user-defined policy label to invoke if the policy evaluates to TRUE.
name	<String>	Read-write	Name for the virtual server. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at sign (@), equal sign (=), and hyphen (-) characters. Can be changed after the virtual server is created.

CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my vserver" or 'my vserver'). .

Minimum length = 1

Possible values = reqvserver, resvserver, policylabel

```
</td></tr><tr><td>priority

</td><td>&lt;Integer&gt;

</td><td>Read-write

</td><td>Priority.

</td></tr><tr><td>bindpoint

</td><td>&lt;String&gt;

</td><td>Read-write

</td><td>Bind point to which to bind the policy.

 <p>Possible values = REQUEST, RESPONSE, MQTT_JUMBO_REQ</p>

</td></tr><tr><td>__count

</td><td>&lt;Double&gt;

</td><td>Read-write

</td><td>count parameter

</td></tr></tbody></table>
```

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/lbvserver_tmtrafficpolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"lbvserver_tmtrafficpolicy_binding":{

<b>"name":<String_value>,
```

```
</b>"policyname":<String_value>,

"priority":<Integer_value>,

"gotopriorityexpression":<String_value>,

"bindpoint":<String_value>,

"invoke":<Boolean_value>,

"labeltype":<String_value>,

"labelname":<String_value>,

"order":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_tmtrafficpolicy_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ lbvserver_tmtrafficpolicy_binding/ name_value<String> ? **args=policyname: <String_value> ,bindpoint: <String_value> ,priority: <Integer_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_tmtrafficpolicy_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ lbvserver_tmtrafficpolicy_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of lbvserver_tmtrafficpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_tmtrafficpolicy_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the lbvserver_tmtrafficpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lbvserver_tmtrafficpolicy_binding": [ {

"policyname":<String_value>,

"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>,

"order":<Integer_value>,

"labelname":<String_value>,
```

```
"name":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"bindpoint":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_tmtrafficpolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_tmtrafficpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lbvserver_tmtrafficpolicy_binding": [ {

"policyname":<String_value>,
```

```
"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>,

"order":<Integer_value>,

"labelname":<String_value>,

"name":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"bindpoint":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_tmtrafficpolicy_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"lbvserver_tmtrafficpolicy_binding": [ { "__count": "#no"} ] }
```

lbvserver_transformpolicy_binding

Binding object showing the transformpolicy that can be bound to lbvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
invoke	<Boolean>	Read-write	Invoke policies bound to a virtual server or policy label.
gotopriorityexpression	<String>	Read-write	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
policyname	<String>	Read-write	Name of the policy bound to the LB vserver.
name	<String>	Read-write	Name for the virtual server. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at sign (@), equal sign (=), and hyphen (-) characters. Can be changed after the virtual server is created.

CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my vserver" or 'my vserver'). .

Minimum length = 1

Possible values = reqvserver, resvserver, policylabel

Possible values = REQUEST, RESPONSE, MQTT_JUMBO_REQ

Minimum value = 1

Maximum value = 8192

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/lbvserver_transformpolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"lbvserver_transformpolicy_binding":{

<b>"name":<String_value>,

</b>"policyname":<String_value>,

"priority":<Integer_value>,

"gotopriorityexpression":<String_value>,

"bindpoint":<String_value>,

"invoke":<Boolean_value>,

"labeltype":<String_value>,

"labelname":<String_value>,

"order":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_transformpolicy_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ lbvserver_transformpolicy_binding/ name_value<String> ? **args=policyname: <String_value> ,bindpoint: <String_value> ,priority: <Integer_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_transformpolicy_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ lbvserver_transformpolicy_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of lbvserver_transformpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_transformpolicy_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the lbvserver_transformpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lbvserver_transformpolicy_binding": [ {

"invoke":<Boolean_value>,

"gotopriorityexpression":<String_value>,

"policyname":<String_value>,

"name":<String_value>,

"priority":<Integer_value>,

"labeltype":<String_value>,

"bindpoint":<String_value>,

"labelname":<String_value>,

"order":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_transformpolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_transformpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lbvserver_transformpolicy_binding": [ {

"invoke":<Boolean_value>,

"gotopriorityexpression":<String_value>,

"policyname":<String_value>,

"name":<String_value>,

"priority":<Integer_value>,

"labeltype":<String_value>,

"bindpoint":<String_value>,

"labelname":<String_value>,

"order":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_transformpolicy_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"lbvserver_transformpolicy_binding": [ { "__count": "#no"} ] }
```

lbvserver_videooptimizationdetectionpolicy_binding

Binding object showing the videooptimizationdetectionpolicy that can be bound to lbvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
order	<Integer>	Read-write	Integer specifying the order of the service. A larger number specifies a lower order. Defines the order of the service relative to the other services in the load balancing vserver's bindings.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Determines the priority given to the service among all the services bound. Minimum value = 1 Maximum value = 8192
labelname	<String>	Read-write	Name of the label invoked.
name	<String>	Read-write	Name for the virtual server. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at sign (@), equal sign (=), and hyphen (-) characters. Can be changed after the virtual server is created.

CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my vserver" or 'my vserver'). .

Minimum length = 1

Possible values = REQUEST, RESPONSE, MQTT_JUMBO_REQ

Possible values = reqvserver, resvserver, policylabel

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/ lbvserver_videooptimizationdetectionpolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"lbvserver_videooptimizationdetectionpolicy_binding":{

<b>"name":<String_value>,

</b>"policyname":<String_value>,

"priority":<Integer_value>,

"gotopriorityexpression":<String_value>,

"bindpoint":<String_value>,

"invoke":<Boolean_value>,

"labeltype":<String_value>,

"labelname":<String_value>,

"order":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/ lbvserver_videooptimizationdetectionpolicy_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ lbvserver_videooptimizationdetectionpolicy_binding/ name_value<String> ? **args=policyname: <String_value> ,bindpoint: <String_value> ,priority: <Integer_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/ lbvserver_videooptimizationdetectionpolicy_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ lbvserver_videooptimizationdetectionpolicy_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of lbvserver_videooptimizationdetectionpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ lbvserver_videooptimizationdetectionpolicy_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the lbvserver_videooptimizationdetectionpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lbvserver_videooptimizationdetectionpolicy_binding": [ {

"order":<Integer_value>,

"labelname":<String_value>,

"name":<String_value>,

"bindpoint":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"policyname":<String_value>,

"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/ lbvserver_videooptimizationdetectionpolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ lbvserver_videooptimizationdetectionpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lbvserver_videooptimizationdetectionpolicy_binding": [ {

"order":<Integer_value>,

"labelname":<String_value>,

"name":<String_value>,

"bindpoint":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"policyname":<String_value>,

"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/ lbvserver_videooptimizationdetectionpolicy_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"lbvserver_videooptimizationdetectionpolicy_binding": [ { "__count":
"#no"} ] }
```

lbvserver_videooptimizationpacingpolicy_binding

Binding object showing the videooptimizationpacingpolicy that can be bound to lbvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
policyname	<String>	Read-write	Name of the policy bound to the LB vserver.
invoke	<Boolean>	Read-write	Invoke policies bound to a virtual server or policy label.
gotopriorityexpression	<String>	Read-write	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
order	<Integer>	Read-write	Integer specifying the order of the service. A larger

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			number specifies a lower order. Defines the order of the service relative to the other services in the load balancing vserver's bindings. Determines the priority given to the service among all the services bound. Minimum value = 1 Maximum value = 8192
labelname	<String>	Read-write	Name of the label invoked.
bindpoint	<String>	Read-write	The bindpoint to which the policy is bound. Possible values = REQUEST, RESPONSE, MQTT_JUMBO_REQ
priority	<Integer>	Read-write	Priority.
labeltype	<String>	Read-write	The invocation type. Possible values = reqvserver, resvserver, policylabel
name	<String>	Read-write	Name for the virtual server. Must begin with an ASCII alphanumeric or

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at sign (@), equal sign (=), and hyphen (-) characters. Can be changed after the virtual server is created.

CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my vserver" or 'my vserver'). .

Minimum length = 1

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/lbvserver_videooptimizationpacingpolicy_binding
HTTP Method: PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"lbvserver_videooptimizationpacingpolicy_binding":{

<b>"name":<String_value>,

</b>"policyname":<String_value>,

"priority":<Integer_value>,

"gotopriorityexpression":<String_value>,

"bindpoint":<String_value>,
```

```
"invoke":<Boolean_value>,

"labeltype":<String_value>,

"labelname":<String_value>,

"order":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_videooptimizationpacingpolicy_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_videooptimizationpacingpolicy_binding/ name_value<String> ? **args=policyname: <String_value> ,bindpoint: <String_value> ,priority: <Integer_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_videooptimizationpacingpolicy_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_videooptimizationpacingpolicy_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of lbvserver_videooptimizationpacingpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ lbvserver_videooptimizationpacingpolicy_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the lbvserver_videooptimizationpacingpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lbvserver_videooptimizationpacingpolicy_binding": [ {

"policyname":<String_value>,

"invoke":<Boolean_value>,

"gotopriorityexpression":<String_value>,

"order":<Integer_value>,

"labelname":<String_value>,

"bindpoint":<String_value>,

"priority":<Integer_value>,
```

```
"labeltype":<String_value>,

"name":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/ lbvserver_videooptimizationpacingpolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ lbvserver_videooptimizationpacingpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lbvserver_videooptimizationpacingpolicy_binding": [ {

"policyname":<String_value>,

"invoke":<Boolean_value>,

"gotopriorityexpression":<String_value>,
```

```
"order":<Integer_value>,

"labelname":<String_value>,

"bindpoint":<String_value>,

"priority":<Integer_value>,

"labeltype":<String_value>,

"name":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/ lbvserver_videooptimizationpacingpolicy_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"lbvserver_videooptimizationpacingpolicy_binding": [ { "__count":
"#no"} ] }
```

lbwlm

Configuration for web log manager resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
wlmname	<String>	Read-write	The name of the Work Load Manager. Minimum length = 1
ipaddress	<String>	Read-write	The IP address of the WLM.
port	<Integer>	Read-write	The port of the WLM. Range 1 - 65535 * in CLI is represented as 65535 in NITRO API
lbuid	<String>	Read-write	The LBUID for the Load Balancer to communicate to the Work Load Manager.
katimeout	<Integer>	Read-write	The idle time period after which Citrix ADC would probe the WLM. The value ranges from 1 to 1440 minutes. Default value: 2 Minimum value = 0 Maximum value = 1440

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
secure	<String>	Read-only	Use this parameter to enable secure mode of communication with WLM. Possible values = YES, NO
state	<String>	Read-only	State of the WLM. Possible values = ACTIVE, INACTIVE, UNKNOWN
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbwlm **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"lbwlm":{

<b>"wlmname":<String_value>,

</b>"ipaddress":<String_value>,

"port":<Integer_value>,

<b>"lbuid":<String_value>,

</b>"katimeout":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbwlm/ wlmname_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbwlm **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"lbwlm":{

<b>"wlmname":<String_value>,

</b>"katimeout":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbwlm? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"lbwlm":{

<b>"wlmname":<String_value>,

</b>"katimeout":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbwlm **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/lbwlm? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/lbwlm? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of lbwlm resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/lbwlm? **view=summary**

Use this query-parameter to get the summary output of lbwlm resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/lbwlm? **pagesize=#no;pageno=#no**

Use this query-parameter to get the lbwlm resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "lbwlm": [ {

"wlmname":<String_value>,

"ipaddress":<String_value>,

"port":<Integer_value>,

"secure":<String_value>,

"katimeout":<Integer_value>,

"lbuid":<String_value>,

"state":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbwlm/ wlmname_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/lbwlm/ wlmname_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/lbwlm/ wlmname_value<String> ? **view=summary**

Use this query-parameter to get the summary output of lbwlm resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lbwlm": [ {

"wlmname":<String_value>,

"ipaddress":<String_value>,

"port":<Integer_value>,

"secure":<String_value>,
```

```
"katimeout":<Integer_value>,

"lbuid":<String_value>,

"state":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbwlm? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "lbwlm": [ { "__count": "#no"} ] }
```

lbwlm_binding

Binding object which returns the resources bound to lbwlm.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
wlmname	<String>	Read-write	The name of the work load manager. Minimum length = 1
lbwlm_lbvserver_binding	<lbwlm_lbvserver_binding[]>	Read-only	lbvserver that can be bound to lbwlm.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbwlm_binding/ wlmname_value<String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "lbwlm_binding": [ {

"wlmname":<String_value>,

"lbwlm_lbvserver_binding":<lbwlm_lbvserver_binding[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbwlm_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/lbwlm_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "lbwlm_binding": [ {

"wlmname":<String_value>,

"lbwlm_lbvserver_binding":<lbwlm_lbvserver_binding[]_value>

}]}
```

lbwlm_lbvserver_binding

Binding object showing the lbvserver that can be bound to lbwlm.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
wlmname	<String>	Read-write	The name of the Work Load Manager. Minimum length = 1
vservername	<String>	Read-write	Name of the virtual server which is to be bound to the WLM.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT
- ADD
- DELETE

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/lbwlm_lbvserver_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"lbwlm_lbvserver_binding":{

<b>"wlmname":<String_value>,

</b><b>"vservername":<String_value></b>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbwlm_lbvserver_binding/ wlmname_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ lbwlm_lbvserver_binding/ wlmname_value<String> ? **args= vservername:<String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbwlm_lbvserver_binding/ wlmname_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/

lbwlm_lbvserver_binding/ wlmname_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of lbwlm_lbvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/lbwlm_lbvserver_binding/ wlmname_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the lbwlm_lbvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lbwlm_lbvserver_binding": [ {

"wlmname":<String_value>,

"vservername":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbwlm_lbvserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/lbwlm_lbvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lbwlm_lbvserver_binding": [ {

"wlmname":<String_value>,

"vservername":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbwlm_lbvserver_binding/wlmname_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"lbwlm_lbvserver_binding": [ { "__count": "#no"} ] }
```

lldp

LLDP

Link Layer Discovery Protocol.

NAME	DESCRIPTION
lldpneighbors	Configuration for lldp neighbors
lldpparam	Configuration for lldp params

lldpneighbors

Configuration for lldp neighbors resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ifnum	<String>	Read-write	Interface Name.
nodeid	<Integer>	Read-write	Unique number that identifies the cluster node. Minimum value = 0

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum value = 31
chassisidsubtype	<String>	Read-only	Chassis id sub type. Possible values = NONE, Component, Interface Alias, Port Component, MAC Address, Network Address, Interface Name, Locally Assigned
chassisid	<String>	Read-only	Chassis Id.
portidsubtype	<String>	Read-only	Port id subtype. Possible values = NONE, Interface Alias, Port Component, MAC Address, Network Address, Interface Name, Agent Circuit ID, Locally Assigned
portid	<String>	Read-only	Port Id.
ttl	<Integer>	Read-only	Time to Live.
portdescription	<String>	Read-only	Port Description.
sys	<String>	Read-only	System Name.
sysdesc	<String>	Read-only	System Description.
mgmtaddresssubtype	<String>	Read-only	Management Address Type. Possible values = OTHER, IPv4, IPv6

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
mgmtaddress	<String>	Read-only	Management Address.
iftype	<String>	Read-only	Interface subtype. Possible values = UNKNOWN, ifIndex, system port number
ifnumber	<Integer>	Read-only	Interface Number.
vlan	<String>	Read-only	vlan name.
vlanid	<Integer>	Read-only	Vlan Id.
portprotosupported	<Integer>	Read-only	Flag to show Port Protocol Support.
portprotoenabled	<Integer>	Read-only	Flag to show Port Protocol support enabled.
portprotoid	<Integer>	Read-only	Port Protocol ID.
portvlanid	<Integer>	Read-only	Port Vlan Id.
protocolid	<String>	Read-only	port vlan id name.
linkaggrcapable	<String>	Read-only	Is neighbor Link Aggregation Capable. Possible values = NO, YES
linkaggrenabled	<String>	Read-only	Is link aggregation Enabled. Possible values = NO, YES
linkaggrid	<Integer>	Read-only	Link Aggregation Id.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
flag	<Integer>	Read-only	.
syscapabilities	<String>	Read-only	Acronyms for remote system capabilities: OT : Other. RE : Repeater(IETF RFC 2108). BR : MAC Bridge(IEEE Std 802.1D). WL : WLAN Access Point(IEEE Std 802.11 MIB). RO : ROuter(IETF RFC 1812). TE : Telephone(IETF RFC 4293). DO : DOCSIS cable device(IETF RFC 4639 and IETF RFC 4546). ST : STation only(IETF RFC 4293). CV : C-VLAN component of a VLAN Bridge(IEEE Std 802.1Q).

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			SV : S-VLAN component of a VLAN Bridge(IEEE Std 802.1Q). MR : Two port MAC Relay(IEEE Std 802.1Q).
syscapenabled	<String>	Read-only	Acronyms for remote system enabled capabilities: OT : Other. RE : Repeater(IETF RFC 2108). BR : MAC Bridge(IEEE Std 802.1D). WL : WLAN Access Point(IEEE Std 802.11 MIB). RO : ROuter(IETF RFC 1812). TE : Telephone(IETF RFC 4293). DO : DOCSIS cable device(IETF RFC 4639 and IETF RFC 4546).

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			ST : STation only(IETF RFC 4293). CV : C-VLAN component of a VLAN Bridge(IEEE Std 802.1Q). SV : S-VLAN component of a VLAN Bridge(IEEE Std 802.1Q). MR : Two port MAC Relay(IEEE Std 802.1Q).
autonegsupport	<String>	Read-only	MAC/PHY autonegotiation support. Possible values = NO, YES
autonegenabled	<String>	Read-only	MAC/PHY autonegotiation enabled. Possible values = NO, YES
autonegadvertised	<String>	Read-only	MAC/PHY autonegotiation advetised.
autonegmautype	<String>	Read-only	MAC/PHY Medium Attachment Unit (MAU) type of the port. Description listed below:

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			AUI - no internal MAU, view from AUI 10Base5 - thick coax MAU Foirl - FOIRL MAU 10Base2 - thin coax MAU 10BaseT - UTP MAU 10BaseFP - passive fiber MAU 10BaseFB - sync fiber MAU 10BaseFL - async fiber MAU 10Broad36 - broadband DTE MAU 10BaseTHD - UTP MAU, half duplex mode 10BaseTFD - UTP MAU, full duplex mode 10BaseFLHD - async fiber MAU, half duplex mode

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			10BaseFLDF - async fiber MAU, full duplex mode 10BaseT4 - 4 pair category 3 UTP 100BaseTXHD - 2 pair category 5 UTP, half duplex mode 100BaseTXFD - 2 pair category 5 UTP, full duplex mode 100BaseFXHD - X fiber over PMT, half duplex mode 100BaseFXFD - X fiber over PMT, full duplex mode 100BaseT2HD - 2 pair category 3 UTP, half duplex mode 100BaseT2DF - 2 pair category 3 UTP, full duplex mode 1000BaseXHD - PCS/PMA,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			unknown PMD, half duplex mode 1000BaseXFD - PCS/PMA, unknown PMD, full duplex mode 1000BaseLXHD - Fiber over long-wavelength laser, half duplex mode 1000BaseLXFD - Fiber over long-wavelength laser, full duplex mode 1000BaseSXHD - Fiber over short-wavelength laser, half duplex mode 1000BaseSXFD - Fiber over short-wavelength laser, full duplex mode 1000BaseCXHD - Copper over 150-Ohm balanced cable, half duplex mode 1000BaseCXFD - Copper over 150-Ohm balanced

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			cable, full duplex mode 1000BaseTHD - Four-pair Category 5 UTP, half duplex mode 1000BaseTFD - Four-pair Category 5 UTP, full duplex mode 10GigBaseX - X PCS/PMA, unknown PMD 10GigBaseLX4 - X fiber over WWDM optics 10GigBaseR - R PCS/PMA, unknown PMD 10GigBaseER - R fiber over 1550 nm optics 10GigBaseLR - R fiber over 1310 nm optics 10GigBaseSR - R fiber over 850 nm optics

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			10GigBaseW - W PCS/PMA, unknown PMD 10GigBaseEW - W fiber over 1550 nm optics 10GigBaseLW - W fiber over 1310 nm optics 10GigBaseSW - W fiber over 850 nm optics. Possible values = Not Recieved, AUI, 10Base5, Foirl, 10Base2, 10BaseT, 10BaseFP, 10BaseFB, 10BaseFL, 10Broad36, 10BaseTHD, 10BaseTFD, 10BaseFLHD, 10BaseFLDF, 10BaseT4, 100BaseTXHD, 100BaseTXFD, 100BaseFXHD, 100BaseFXFD, 100BaseT2HD, 100BaseT2DF, 1000BaseXHD, 1000BaseXFD,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			1000BaseLXHD, 1000BaseLXFD, 1000BaseSXHD, 1000BaseSXFD, 1000BaseCXHD, 1000BaseCXFD, 1000BaseTHD, 1000BaseTFD, 10GigBaseX, 10GigBaseLX4, 10GigBaseR, 10GigBaseER, 10GigBaseLR, 10GigBaseSR, 10GigBaseW, 10GigBaseEW, 10GigBaseLW, 10GigBaseSW
mtu	<Integer>	Read-only	MTU of Remote Device.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET (ALL)
- GET
- COUNT
- CLEAR

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

CLEAR

URL: http:// <netscaler-ip-address> /nitro/v1/config/lldpneighbors? **action=clear HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"lldpneighbors":{

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/lldpneighbors **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/lldpneighbors? **args=ifnum: <String_value> ,nodeid: <Integer_value>**

Use this query-parameter to get lldpneighbors resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/config/lldpneighbors? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/lldpneighbors? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of lldpneighbors resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/lldpneighbors? **view=summary**

Use this query-parameter to get the summary output of lldpneighbors resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/lldpneighbors? **pagesize=#no;pageno=#no**

Use this query-parameter to get the lldpneighbors resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "lldpneighbors": [ {

ifnum:<String_value>,nodeid:<Integer_value>"chassisidsubtype":<String_valu
e>,

"chassisid":<String_value>,

"portidsubtype":<String_value>,

"portid":<String_value>,

"ttl":<Integer_value>,

"portdescription":<String_value>,

"sys":<String_value>,

"sysdesc":<String_value>,

"mgmtaddresssubtype":<String_value>,

"mgmtaddress":<String_value>,

"iftype":<String_value>,

"ifnumber":<Integer_value>,

"vlan":<String_value>,

"vlanid":<Integer_value>,

"portprotosupported":<Integer_value>,

"portprotoenabled":<Integer_value>,
```

```
"portprotoid":<Integer_value>,

"portvlanid":<Integer_value>,

"protocolid":<String_value>,

"linkaggrcapable":<String_value>,

"linkaggrenabled":<String_value>,

"linkaggrid":<Integer_value>,

"flag":<Integer_value>,

"syscapabilities":<String_value>,

"syscapenabled":<String_value>,

"autonegsupport":<String_value>,

"autonegenabled":<String_value>,

"autonegadvertised":<String_value>,

"autonegmautype":<String_value>,

"mtu":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lldpneighbors/ ifnum_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/lldpneighbors/ ifnum_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/lldpneighbors/ ifnum_value<String> ? **view=summary**

Use this query-parameter to get the summary output of lldpneighbors resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lldpneighbors": [ {

ifnum:<String_value>,nodeid:<Integer_value>"chassisidsubtype":<String_valu
e>,

"chassisid":<String_value>,

"portidsubtype":<String_value>,

"portid":<String_value>,

"ttl":<Integer_value>,

"portdescription":<String_value>,

"sys":<String_value>,

"sysdesc":<String_value>,

"mgmtaddresssubtype":<String_value>,
```

```
"mgmtaddress":<String_value>,

"iftype":<String_value>,

"ifnumber":<Integer_value>,

"vlan":<String_value>,

"vlanid":<Integer_value>,

"portprotosupported":<Integer_value>,

"portprotoenabled":<Integer_value>,

"portprotoid":<Integer_value>,

"portvlanid":<Integer_value>,

"protocolid":<String_value>,

"linkaggrcapable":<String_value>,

"linkaggrenabled":<String_value>,

"linkaggrid":<Integer_value>,

"flag":<Integer_value>,

"syscapabilities":<String_value>,

"syscapenabled":<String_value>,

"autonegsupport":<String_value>,

"autonegenabled":<String_value>,

"autonegadvertised":<String_value>,

"autonegmautype":<String_value>,

"mtu":<Integer_value>,

"_nextgenapiresource":<String_value>
```

```
}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/lldpneighbors? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "lldpneighbors": [ { "__count": "#no"} ] }
```

lldpparam

Configuration for lldp params resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
holdtimetxmult	<Integer>	Read-write	A multiplier for calculating the duration for which the receiving device stores the LLDP information in its

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			database before discarding or removing it. The duration is calculated as the holdtimeTxMult (Holdtime Multiplier) parameter value multiplied by the timer (Timer) parameter value. Default value: 4 Minimum value = 1 Maximum value = 20
timer	<Integer>	Read-write	Interval, in seconds, between LLDP packet data units (LLDPDUs). that the Citrix ADC sends to a directly connected device. Default value: 30 Minimum value = 1 Maximum value = 3000
mode	<String>	Read-write	Global mode of Link Layer Discovery Protocol (LLDP) on the Citrix ADC. The resultant LLDP mode of an interface depends on the LLDP mode configured at the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			global and the interface levels. Possible values = NONE, TRANSMITTER, RECEIVER, TRANSCEIVER
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- UPDATE
- UNSET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/lldpparam **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"lldpparam":{

"holdtimetxmult":<Integer_value>,

"timer":<Integer_value>,

"mode":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lldpparam? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"lldpparam":{

"holdtimetxmult":true,

"timer":true,

"mode":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/lldpparam **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "lldpparam": [ {

"holdtimetxmult":<Integer_value>,

"timer":<Integer_value>,

"mode":<String_value>,
```

```
"_nextgenapiresource":<String_value>

}]}
```

lsn

Lsn

Large Scale NAT commands

NAME	DESCRIPTION
lsnappsattributes	Configuration for LSN Application Attributes
lsnappsprofile	Configuration for LSN Application Profile
lsnappsprofile_binding	Binding object showing the resources that can be bound to lsnappsprofile
lsnappsprofile_lsnappsattributes_binding	Binding object showing the lsnappsattributes that can be bound to lsnappsprofile
lsnappsprofile_port_binding	Binding object showing the port that can be bound to lsnappsprofile
lsnclient	Configuration for lsn client
lsnclient_binding	Binding object showing the resources that can be bound to lsnclient
lsnclient_network6_binding	Binding object showing the network6 that can be bound to lsnclient

NAME	DESCRIPTION
lsnclient_network_binding	Binding object showing the network that can be bound to lsnclient
lsnclient_nsacl6_binding	Binding object showing the nsacl6 that can be bound to lsnclient
lsnclient_nsacl_binding	Binding object showing the nsacl that can be bound to lsnclient
lsndeterministicnat	Configuration for deterministic NAT
lsngroup	Configuration for LSN group
lsngroup_binding	Binding object showing the resources that can be bound to lsngroup
lsngroup_ipsecalgprofile_binding	Binding object showing the ipsecalgprofile that can be bound to lsngroup
lsngroup_lsnappsprofile_binding	Binding object showing the lsnappsprofile that can be bound to lsngroup
lsngroup_lsnhttphdrlogprofile_binding	Binding object showing the lsnhttphdrlogprofile that can be bound to lsngroup
lsngroup_lsnlogprofile_binding	Binding object showing the lsnlogprofile that can be bound to lsngroup
lsngroup_lsnpool_binding	Binding object showing the lsnpool that can be bound to lsngroup

NAME	DESCRIPTION
lsngroup_lsnrtspalgprofile_binding	Binding object showing the lsnrtspalgprofile that can be bound to lsngroup
lsngroup_lsnsipalgprofile_binding	Binding object showing the lsnsipalgprofile that can be bound to lsngroup
lsngroup_lsntransportprofile_binding	Binding object showing the lsntransportprofile that can be bound to lsngroup
lsngroup_pcpserver_binding	Binding object showing the pcpserver that can be bound to lsngroup
lsnhttphdrlogprofile	Configuration for LSN HTTP header logging Profile
lsnip6profile	Configuration for LSN ip6 Profile
lsnlogprofile	Configuration for LSN logging Profile
lsnparameter	Configuration for LSN parameter
lsnpool	Configuration for LSN pool
lsnpool_binding	Binding object showing the resources that can be bound to lsnpool
lsnpool_lsnip_binding	Binding object showing the lsnip that can be bound to lsnpool

NAME	DESCRIPTION
lsnrtspalgprofile	Configuration for LSN RTSPALG Profile
lsnrtspalgsession	Configuration for LSN RTSPALG session
lsnrtspalgsession_binding	Binding object showing the resources that can be bound to lsnrtspalgsession
lsnrtspalgsession_datachannel_binding	Binding object showing the datachannel that can be bound to lsnrtspalgsession
lsnsession	Configuration for lsn session
lsnsipalgcall	Configuration for LSN SIPALG call
lsnsipalgcall_binding	Binding object showing the resources that can be bound to lsnsipalgcall
lsnsipalgcall_controlchannel_binding	Binding object showing the controlchannel that can be bound to lsnsipalgcall
lsnsipalgcall_datachannel_binding	Binding object showing the datachannel that can be bound to lsnsipalgcall
lsnsipalgprofile	Configuration for LSN SIPALG Profile
lsnstatic	Configuration for static mapping
lsntransportprofile	Configuration for LSN Transport Profile

lsnappsattributes

Configuration for LSN Application Attributes resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the LSN Application Port ATTRIBUTES. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the LSN application profile is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "lsn application profile1" or 'lsn application profile1'). Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum length = 127
transportprotocol	<String>	Read-write	Name of the protocol(TCP,UDP) for which the parameters of this LSN application port ATTRIBUTES applies. Possible values = TCP, UDP, ICMP
port	<String>	Read-write	This is used for Displaying Port/Port range in CLI/ Nitro.Lowport, Highport values are populated and used for displaying.Port numbers or range of port numbers to match against the destination port of the incoming packet from a subscriber. When the destination port is matched, the LSN application profile is applied for the LSN session. Separate a range of ports with a hyphen. For example, 40-90. Minimum length = 1
sessiontimeout	<Integer>	Read-write	Timeout, in seconds, for an idle LSN session. If an LSN session is idle for a time that exceeds

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			this value, the Citrix ADC removes the session.This timeout does not apply for a TCP LSN session when a FIN or RST message is received from either of the endpoints. Default value: 30 Minimum value = 5 Maximum value = 600
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnappsattributes **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"lsnappsattributes":{

<b>"name":<String_value>,

</b><b>"transportprotocol":<String_value>,

</b>"port":<String_value>,

"sessiontimeout":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnappsattributes/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnappsattributes **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"lsnappsattributes":{

<b>"name":<String_value>,

</b>"sessiontimeout":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnappsattributes? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"lsnappsattributes":{

<b>"name":<String_value>,

</b>"sessiontimeout":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnappsattributes **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/lsnappsattributes? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/lsnappsattributes? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of lsnappsattributes resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/lsnappsattributes? **view=summary**

Use this query-parameter to get the summary output of lsnappsattributes resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/lsnappsattributes? **pagesize=#no;pageno=#no**

Use this query-parameter to get the lsnappsattributes resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "lsnappsattributes": [ {

"name":<String_value>,

"transportprotocol":<String_value>,

"sessiontimeout":<Integer_value>,

"port":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnappsattributes/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/lsnappsattributes/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/lsnappsattributes/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of lsnappsattributes resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lsnappsattributes": [ {

"name":<String_value>,

"transportprotocol":<String_value>,

"sessiontimeout":<Integer_value>,

"port":<String_value>,
```

```
"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnappsattributes? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "lsnappsattributes": [ { "__count": "#no"} ] }
```

lsnappsprofile

Configuration for LSN Application Profile resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
appsprofilename	<String>	Read-write	Name for the LSN application profile. Must begin with an ASCII alphanumeric

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the LSN application profile is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "lsn application profile1" or 'lsn application profile1'). Minimum length = 1 Maximum length = 127
transportprotocol	<String>	Read-write	Name of the protocol for which the parameters of this LSN application profile applies. Possible values = TCP, UDP, ICMP

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ippooling	<String>	Read-write	NAT IP address allocation options for sessions associated with the same subscriber. Available options function as follows: * Paired - The Citrix ADC allocates the same NAT IP address for all sessions associated with the same subscriber. When all the ports of a NAT IP address are used in LSN sessions (for same or multiple subscribers), the Citrix ADC ADC drops any new connection from the subscriber. * Random - The Citrix ADC allocates random NAT IP addresses, from the pool, for different sessions associated with the same subscriber. This parameter is applicable to

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			dynamic NAT allocation only. Default value: RANDOM Possible values = PAIRED, RANDOM
mapping	<String>	Read-write	Type of LSN mapping to apply to subsequent packets originating from the same subscriber IP address and port. Consider an example of an LSN mapping that includes the mapping of the subscriber IP:port (X:x), NAT IP:port (N:n), and external host IP:port (Y:y). Available options function as follows: * ENDPOINT-INDEPENDENT - Reuse the LSN mapping for subsequent packets sent from the same subscriber IP address and port

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			(X:x) to any external IP address and port. * ADDRESS-DEPENDENT - Reuse the LSN mapping for subsequent packets sent from the same subscriber IP address and port (X:x) to the same external IP address (Y), regardless of the external port. * ADDRESS-PORT-DEPENDENT - Reuse the LSN mapping for subsequent packets sent from the same internal IP address and port (X:x) to the same external IP address and port (Y:y) while the mapping is still active. Default value: ADDRESS-PORT-DEPENDENT Possible values = ENDPOINT-INDEPENDENT,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			ADDRESS-DEPENDENT, ADDRESS-PORT-DEPENDENT
filtering	<String>	Read-write	Type of filter to apply to packets originating from external hosts. Consider an example of an LSN mapping that includes the mapping of subscriber IP:port (X:x), NAT IP:port (N:n), and external host IP:port (Y:y). Available options function as follows: * ENDPOINT INDEPENDENT - Filters out only packets not destined to the subscriber IP address and port X:x, regardless of the external host IP address and port source (Z:z). The Citrix ADC forwards any packets destined to X:x. In other words, sending packets

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			from the subscriber to any external IP address is sufficient to allow packets from any external hosts to the subscriber. * ADDRESS DEPENDENT - Filters out packets not destined to subscriber IP address and port X:x. In addition, the ADC filters out packets from Y:y destined for the subscriber (X:x) if the client has not previously sent packets to Y:anyport (external port independent). In other words, receiving packets from a specific external host requires that the subscriber first send packets to that specific external host's IP address. * ADDRESS PORT DEPENDENT (the default) - Filters out

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			packets not destined to subscriber IP address and port (X:x). In addition, the Citrix ADC filters out packets from Y:y destined for the subscriber (X:x) if the subscriber has not previously sent packets to Y:y. In other words, receiving packets from a specific external host requires that the subscriber first send packets first to that external IP address and port. Default value: ADDRESS-PORT-DEPENDENT Possible values = ENDPOINT-INDEPENDENT, ADDRESS-DEPENDENT, ADDRESS-PORT-DEPENDENT
tcpproxy	<String>	Read-write	Enable TCP proxy, which enables the Citrix ADC to

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			optimize the TCP traffic by using Layer 4 features. Default value: DISABLED Possible values = ENABLED, DISABLED
td	<Integer>	Read-write	ID of the traffic domain through which the Citrix ADC sends the outbound traffic after performing LSN. If you do not specify an ID, the ADC sends the outbound traffic through the default traffic domain, which has an ID of 0. Default value: 4095
l2info	<String>	Read-write	Enable l2info by creating natpcbs for LSN, which enables the Citrix ADC to use L2CONN/MBF with LSN. Default value: DISABLED Possible values = ENABLED, DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnappsprofile **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"lsnappsprofile":{

<b>"appsprofilename":<String_value>,

</b><b>"transportprotocol":<String_value>,

</b>"ippooling":<String_value>,

"mapping":<String_value>,

"filtering":<String_value>,

"tcpproxy":<String_value>,

"td":<Integer_value>,

"l2info":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnappsprofile/ appsprofilename_value<String>
HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnappsprofile **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"lsnappsprofile":{

<b>"appsprofilename":<String_value>,

</b>"ippooling":<String_value>,

"mapping":<String_value>,

"filtering":<String_value>,

"tcpproxy":<String_value>,

"td":<Integer_value>,

"l2info":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnappsprofile? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"lsnappsprofile":{

<b>"appsprofilename":<String_value>,

</b>"ippooling":true,

"mapping":true,

"filtering":true,

"tcpproxy":true,

"td":true,

"l2info":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnappsprofile **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/lsnappsprofile? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/lsnappsprofile? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of lsnappsprofile resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/lsnappsprofile? **view=summary**

Use this query-parameter to get the summary output of lsnappsprofile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/lsnappsprofile? **pagesize=#no;pageno=#no**

Use this query-parameter to get the lsnappsprofile resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "lsnappsprofile": [ {

"appsprofilename":<String_value>,

"transportprotocol":<String_value>,

"ippooling":<String_value>,

"mapping":<String_value>,

"filtering":<String_value>,

"tcpproxy":<String_value>,

"td":<Integer_value>,

"l2info":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnappsprofile/ appsprofilename_value<String>
Query-parameters: attrs http:// <netscaler-ip-address> /nitro/v1/config/lsnappsprofile/ appsprofilename_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/lsnappsprofile/ appsprofilename_value<String> ? **view=summary**

Use this query-parameter to get the summary output of lsnappsprofile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lsnappsprofile": [ {

"appsprofilename":<String_value>,

"transportprotocol":<String_value>,

"ippooling":<String_value>,

"mapping":<String_value>,

"filtering":<String_value>,

"tcpproxy":<String_value>,

"td":<Integer_value>,

"l2info":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnappsprofile? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "lsnappsprofile": [ { "__count": "#no"} ] }
```

lsnappsprofile_binding

Binding object which returns the resources bound to lsnappsprofile.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
appsprofilename	<String>	Read-write	Name for the LSN application profile. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the LSN application profile is created. The following

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "lsn application profile1" or 'lsn application profile1'). Minimum length = 1 Maximum length = 127
lsnappsprofile_lsnappsattributes_binding	<lsnappsprofile_lsnappsattributes_binding[]>	Read-only	lsnappsattributes that can be bound to lsnappsprofile.
lsnappsprofile_port_binding	<lsnappsprofile_port_binding[]>	Read-only	port that can be bound to lsnappsprofile.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnappsprofile_binding/ appsprofilename_value<String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "lsnappsprofile_binding": [ {

"appsprofilename":<String_value>,

"lsnappsprofile_lsnappsattributes_binding":<lsnappsprofile_lsnappsattributes_binding[]_value>,
```

```
"lsnappsprofile_port_binding":<lsnappsprofile_port_binding[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnappsprofile_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/lsnappsprofile_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "lsnappsprofile_binding": [ {

"appsprofilename":<String_value>,

"lsnappsprofile_lsnappsattributes_binding":<lsnappsprofile_lsnappsattributes_binding[]_value>,

"lsnappsprofile_port_binding":<lsnappsprofile_port_binding[]_value>

}]}
```

lsnappsprofile_lsnappsattributes_binding

Binding object showing the lsnappsattributes that can be bound to lsnappsprofile.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
appsprofilename	<String>	Read-write	Name for the LSN application profile. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the LSN application profile is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "lsn application profile1" or 'lsn application profile1').

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum length = 1 Maximum length = 127
appsattributesname	<String>	Read-write	Name of the LSN application port ATTRIBUTES command to bind to the specified LSN Appsprofile. Properties of the Appsprofile will be applicable to this APPSATTRIBUTES.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/lsnappsprofile_lsnappsattributes_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"lsnappsprofile_lsnappsattributes_binding":{

<b>"appsprofilename":<String_value>,

</b>"appsattributesname":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnappsprofile_lsnappsattributes_binding/ appsprofilename_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/ config/lsnappsprofile_lsnappsattributes_binding/ appsprofilename_value<String> ? **args=appsattributesname: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnappsprofile_lsnappsattributes_binding/ appsprofilename_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/ config/lsnappsprofile_lsnappsattributes_binding/ appsprofilename_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of lsnappsprofile_lsnappsattributes_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/lsnappsprofile_lsnappsattributes_binding/ appsprofilename_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the lsnappsprofile_lsnappsattributes_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lsnappsprofile_lsnappsattributes_binding": [ {

"appsprofilename":<String_value>,

"appsattributesname":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnappsprofile_lsnappsattributes_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/lsnappsprofile_lsnappsattributes_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lsnappsprofile_lsnappsattributes_binding": [ {

"appsprofilename":<String_value>,

"appsattributesname":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnappsprofile_lsnappsattributes_binding/appsprofilename_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"lsnappsprofile_lsnappsattributes_binding": [ { "__count": "#no"} ] }
```

lsnappsprofile_port_binding

Binding object showing the port that can be bound to lsnappsprofile.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
lsnport	<String>	Read-write	Port numbers or range of port numbers to match against the destination port of the incoming packet from a subscriber. When the destination port is matched, the LSN application profile is applied for the LSN session. Separate a range of ports with a hyphen. For example, 40-90. Minimum length = 1
appsprofilename	<String>	Read-write	Name for the LSN application profile. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the LSN application profile is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			double or single quotation marks (for example, "lsn application profile1" or 'lsn application profile1'). Minimum length = 1 Maximum length = 127
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.
- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/lsnappsprofile_port_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"lsnappsprofile_port_binding":{

<b>"appsprofilename":<String_value>,

</b>"lsnport":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnappsprofile_port_binding/appsprofilename_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/

config/lsnappsprofile_port_binding/ appsprofilename_value<String> ? **args=lsnport: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnappsprofile_port_binding/ appsprofilename_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/ config/lsnappsprofile_port_binding/ appsprofilename_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of lsnappsprofile_port_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/lsnappsprofile_port_binding/ appsprofilename_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the lsnappsprofile_port_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lsnappsprofile_port_binding": [ {

"lsnport":<String_value>,

"appsprofilename":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnappsprofile_port_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/lsnappsprofile_port_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lsnappsprofile_port_binding": [ {

"lsnport":<String_value>,
```

```
"appsprofilename":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnappsprofile_port_binding/ appsprofilename_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"lsnappsprofile_port_binding": [ { "__count": "#no"} ] }
```

lsnclient

Configuration for lsn client resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
clientname	<String>	Read-write	Name for the LSN client entity. Must begin with an ASCII alphanumeric or

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the LSN client is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "lsn client1" or 'lsn client1'). . Minimum length = 1 Maximum length = 127
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- GET (ALL)
- GET

- COUNT
- DELETE

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnclient **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"lsnclient":{

<b>"clientname":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnclient/ clientname_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnclient **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/lsnclient? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/lsnclient? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of lsnclient resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/lsnclient? **view=summary**

Use this query-parameter to get the summary output of lsnclient resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/lsnclient? **pagesize=#no;pageno=#no**

Use this query-parameter to get the lsnclient resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "lsnclient": [ {

"clientname":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnclient/ clientname_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/lsnclient/ clientname_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/lsnclient/ clientname_value<String> ? **view=summary**

Use this query-parameter to get the summary output of lsnclient resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lsnclient": [ {

"clientname":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnclient? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "lsnclient": [ { "__count": "#no"} ] }
```

lsnclient_binding

Binding object which returns the resources bound to lsnclient.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
clientname	<String>	Read-write	Name for the LSN client entity. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the LSN client is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "lsn

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			client1" or 'lsn client1'). . Minimum length = 1 Maximum length = 127
lsnclient_network_binding	<lsnclient_network_binding[]>	Read-only	network that can be bound to lsnclient.
lsnclient_nsacl6_binding	<lsnclient_nsacl6_binding[]>	Read-only	nsacl6 that can be bound to lsnclient.
lsnclient_network6_binding	<lsnclient_network6_binding[]>	Read-only	network6 that can be bound to lsnclient.
lsnclient_nsacl_binding	<lsnclient_nsacl_binding[]>	Read-only	nsacl that can be bound to lsnclient.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnclient_binding/ clientname_value<String>
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "lsnclient_binding": [ {

"clientname":<String_value>,

"lsnclient_network6_binding":<lsnclient_network6_binding[]_value>,

"lsnclient_nsacl_binding":<lsnclient_nsacl_binding[]_value>,

"lsnclient_network_binding":<lsnclient_network_binding[]_value>,

"lsnclient_nsacl6_binding":<lsnclient_nsacl6_binding[]_value>
```

```
}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnclient_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/lsnclient_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "lsnclient_binding": [ {

"clientname":<String_value>,

"lsnclient_network6_binding":<lsnclient_network6_binding[]_value>,

"lsnclient_nsacl_binding":<lsnclient_nsacl_binding[]_value>,

"lsnclient_network_binding":<lsnclient_network_binding[]_value>,

"lsnclient_nsacl6_binding":<lsnclient_nsacl6_binding[]_value>

}]}
```

lsnclient_network6_binding

Binding object showing the network6 that can be bound to lsnclient.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
td	<Integer>	Read-write	ID of the traffic domain on which this subscriber or the subscriber network (as specified by the network parameter) belongs. If you do not specify an ID, the subscriber or the subscriber network becomes part of the default traffic domain. Default value: 0 Minimum value = 0 Maximum value = 4094
network6	<String>	Read-write	IPv6 address(es) of the LSN subscriber(s) or subscriber network(s) on whose traffic you want the Citrix ADC to perform Large Scale NAT. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
network	<String>	Read-write	IPv4 address(es) of the LSN subscriber(s) or subscriber network(s) on whose traffic you want the Citrix ADC to perform Large Scale NAT. Minimum length = 1
netmask	<String>	Read-write	Subnet mask for the IPv4 address specified in the Network parameter.
clientname	<String>	Read-write	Name for the LSN client entity. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the LSN client is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "lsn

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			client1" or 'lsn client1'). . Minimum length = 1 Maximum length = 127
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/lsnclient_network6_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"lsnclient_network6_binding":{

<b>"clientname":<String_value>,

</b>"network":<String_value>,

"netmask":<String_value>,

"network6":<String_value>,

"td":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnclient_network6_binding/ clientname_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/

lsnclient_network6_binding/ clientname_value<String> ? **args=network: <String_value> ,netmask: <String_value> ,network6: <String_value> ,td: <Integer_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnclient_network6_binding/ clientname_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ lsnclient_network6_binding/ clientname_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of lsnclient_network6_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/lsnclient_network6_binding/ clientname_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the lsnclient_network6_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lsnclient_network6_binding": [ {

"td":<Integer_value>,

"network6":<String_value>,

"network":<String_value>,

"netmask":<String_value>,

"clientname":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnclient_network6_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/lsnclient_network6_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lsnclient_network6_binding": [ {

"td":<Integer_value>,

"network6":<String_value>,

"network":<String_value>,

"netmask":<String_value>,

"clientname":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnclient_network6_binding/ clientname_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"lsnclient_network6_binding": [ { "__count": "#no"} ] }
```

lsnclient_network_binding

Binding object showing the network that can be bound to lsnclient.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
clientname	<String>	Read-write	Name for the LSN client entity. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the LSN client is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "lsn client1" or 'lsn client1'). . Minimum length = 1 Maximum length = 127
netmask	<String>	Read-write	Subnet mask for the IPv4 address specified in the Network parameter.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
network	<String>	Read-write	IPv4 address(es) of the LSN subscriber(s) or subscriber network(s) on whose traffic you want the Citrix ADC to perform Large Scale NAT. Minimum length = 1
td	<Integer>	Read-write	ID of the traffic domain on which this subscriber or the subscriber network (as specified by the network parameter) belongs. If you do not specify an ID, the subscriber or the subscriber network becomes part of the default traffic domain. Default value: 0 Minimum value = 0 Maximum value = 4094
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)

- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/lsnclient_network_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"lsnclient_network_binding":{
```

```
<b>"clientname":<String_value>,

</b>"network":<String_value>,

"netmask":<String_value>,

"td":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnclient_network_binding/ clientname_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ lsnclient_network_binding/ clientname_value<String> ? **args=network: <String_value> ,netmask: <String_value> ,td: <Integer_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnclient_network_binding/ clientname_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ lsnclient_network_binding/ clientname_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of lsnclient_network_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/lsnclient_network_binding/ clientname_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the lsnclient_network_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lsnclient_network_binding": [ {

"clientname":<String_value>,

"netmask":<String_value>,

"network":<String_value>,

"td":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnclient_network_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/lsnclient_network_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lsnclient_network_binding": [ {

"clientname":<String_value>,

"netmask":<String_value>,

"network":<String_value>,

"td":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnclient_network_binding/clientname_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"lsnclient_network_binding": [ { "__count": "#no"} ] }
```

lsnclient_nsacl6_binding

Binding object showing the nsacl6 that can be bound to lsnclient.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
clientname	<String>	Read-write	Name for the LSN client entity. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the LSN client is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			enclose the name in double or single quotation marks (for example, "lsn client1" or 'lsn client1'). . Minimum length = 1 Maximum length = 127
acl6name	<String>	Read-write	Name of any configured extended ACL6 whose action is ALLOW. The condition specified in the extended ACL6 rule is used as the condition for the LSN client. Minimum length = 1
td	<Integer>	Read-write	ID of the traffic domain on which this subscriber or the subscriber network (as specified by the network parameter) belongs. If you do not specify an ID, the subscriber or the subscriber network becomes part of the default traffic domain. Default value: 0 Minimum value = 0 Maximum value = 4094

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/lsnclient_nsacl6_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"lsnclient_nsacl6_binding":{

<b>"clientname":<String_value>,

</b>"acl6name":<String_value>,

"td":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnclient_nsacl6_binding/ clientname_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ lsnclient_nsacl6_binding/ clientname_value<String> ? **args=acl6name: <String_value> ,td: <Integer_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnclient_nsacl6_binding/ clientname_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ lsnclient_nsacl6_binding/ clientname_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of lsnclient_nsacl6_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/lsnclient_nsacl6_binding/ clientname_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the lsnclient_nsacl6_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lsnclient_nsacl6_binding": [ {

"clientname":<String_value>,

"acl6name":<String_value>,

"td":<Integer_value>
```

```
}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnclient_nsacl6_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/lsnclient_nsacl6_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lsnclient_nsacl6_binding": [ {

"clientname":<String_value>,

"acl6name":<String_value>,

"td":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnclient_nsacl6_binding/ clientname_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"lsnclient_nsacl6_binding": [ { "__count": "#no"} ] }
```

lsnclient_nsacl_binding

Binding object showing the nsacl that can be bound to lsnclient.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
td	<Integer>	Read-write	ID of the traffic domain on which this subscriber or the subscriber network (as specified by the network parameter) belongs. If you do not specify an ID, the subscriber or the subscriber network

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			becomes part of the default traffic domain. Default value: 0 Minimum value = 0 Maximum value = 4094
aclname	<String>	Read-write	Name(s) of any configured extended ACL(s) whose action is ALLOW. The condition specified in the extended ACL rule identifies the traffic from an LSN subscriber for which the Citrix ADC is to perform large scale NAT. . Minimum length = 1
clientname	<String>	Read-write	Name for the LSN client entity. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the LSN client is created. The following

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "lsn client1" or 'lsn client1'). . Minimum length = 1 Maximum length = 127
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/lsnclient_nsacl_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"lsnclient_nsacl_binding":{

<b>"clientname":<String_value>,

</b>"aclname":<String_value>,

"td":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnclient_nsacl_binding/ clientname_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ lsnclient_nsacl_binding/ clientname_value<String> ? **args=aclname: <String_value> ,td: <Integer_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnclient_nsacl_binding/ clientname_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ lsnclient_nsacl_binding/ clientname_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of lsnclient_nsacl_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/lsnclient_nsacl_binding/ clientname_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the lsnclient_nsacl_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lsnclient_nsacl_binding": [ {

"td":<Integer_value>,

"aclname":<String_value>,

"clientname":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnclient_nsacl_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/lsnclient_nsacl_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lsnclient_nsacl_binding": [ {

"td":<Integer_value>,

"aclname":<String_value>,

"clientname":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnclient_nsacl_binding/ clientname_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"lsnclient_nsacl_binding": [ { "__count": "#no"} ] }
```

lsndeterministicnat

Configuration for deterministic NAT resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
clientname	<String>	Read-write	The name of the LSN Client.
network6	<String>	Read-write	IPv6 address of the LSN subscriber or B4 device.
subscrip	<String>	Read-write	The Client IP address.
td	<Integer>	Read-write	The LSN client TD. Default value: 0 Minimum value = 0 Maximum value = 4094
natip	<String>	Read-write	The NAT IP address. Minimum length = 1
natprefix	<String>	Read-only	IPv6 address of the LSN subscriber network(B4-Device) on whose traffic the Citrix ADC perform Large Scale NAT.
subscrip2	<String>	Read-only	The Subscriber IP address.
natip2	<String>	Read-only	The NAT IP address.
firstport	<Integer>	Read-only	The Application Protocol Port of the Profile. Minimum value = 1 Maximum value = 65535

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
lastport	<Integer>	Read-only	The Application Protocol Ending Port of the Profile. Minimum value = 1 Maximum value = 65535
srctd	<Integer>	Read-only	The LSN client TD. Minimum value = 0 Maximum value = 4094
nattype	<String>	Read-only	Type of subscriber info(ex: nat44 or ds-lite). Default value: NAT44 Possible values = NAT44, DS-Lite, NAT64
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsndeterministicnat **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/lsndeterministicnat? **args=clientname: <String_value> ,network6: <String_value> ,subscrip: <String_value> ,td: <Integer_value> ,natip: <String_value>**

Use this query-parameter to get lsndeterministicnat resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/config/lsndeterministicnat? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/lsndeterministicnat? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of lsndeterministicnat resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/lsndeterministicnat? **view=summary**

Use this query-parameter to get the summary output of lsndeterministicnat resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/lsndeterministicnat? **pagesize=#no;pageno=#no**

Use this query-parameter to get the lsndeterministicnat resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "lsndeterministicnat": [ {

clientname:<String_value>,network6:<String_value>,subscrip:<String_value>,
td:<Integer_value>,natip:<String_value>"natprefix":<String_value>,

"subscrip2":<String_value>,

"natip2":<String_value>,

"firstport":<Integer_value>,

"lastport":<Integer_value>,

"srctd":<Integer_value>,

"nattype":<String_value>,
```

```
"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsndeterministicnat? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "lsndeterministicnat": [ { "__count": "#no"} ] }
```

lsngroup

Configuration for LSN group resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
groupname	<String>	Read-write	Name for the LSN group. Must begin with an ASCII alphanumeric or

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the LSN group is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "lsn group1" or 'lsn group1'). Minimum length = 1 Maximum length = 127
clientname	<String>	Read-write	Name of the LSN client entity to be associated with the LSN group. You can associate only one LSN client entity with an LSN group.You cannot remove this association or replace with another LSN client entity

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			once the LSN group is created.
nattype	<String>	Read-write	Type of NAT IP address and port allocation (from the bound LSN pools) for subscribers: Available options function as follows: * Deterministic - Allocate a NAT IP address and a block of ports to each subscriber (of the LSN client bound to the LSN group). The Citrix ADC sequentially allocates NAT resources to these subscribers. The Citrix ADC ADC assigns the first block of ports (block size determined by the port block size parameter of the LSN group) on the beginning NAT IP address to the beginning subscriber IP address. The next range of ports is assigned to the next

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			subscriber, and so on, until the NAT address does not have enough ports for the next subscriber. In this case, the first port block on the next NAT address is used for the subscriber, and so on. Because each subscriber now receives a deterministic NAT IP address and a block of ports, a subscriber can be identified without any need for logging. For a connection, a subscriber can be identified based only on the NAT IP address and port, and the destination IP address and port. The maximum number of LSN subscribers allowed, globally, is 1 million.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			* Dynamic - Allocate a random NAT IP address and a port from the LSN NAT pool for a subscriber's connection. If port block allocation is enabled (in LSN pool) and a port block size is specified (in the LSN group), the Citrix ADC allocates a random NAT IP address and a block of ports for a subscriber when it initiates a connection for the first time. The ADC allocates this NAT IP address and a port (from the allocated block of ports) for different connections from this subscriber. If all the ports are allocated (for different subscriber's connections) from the subscriber's allocated port block, the ADC allocates a

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			new random port block for the subscriber. Default value: DYNAMIC Possible values = DYNAMIC, DETERMINISTIC
allocpolicy	<String>	Read-write	NAT IP and PORT block allocation policy for Deterministic NAT. Supported Policies are, 1: PORTS: Port blocks from single NATIP will be allocated to LSN subscribers sequentially. After all blocks are exhausted, port blocks from next NATIP will be allocated and so on. 2: IPADDRS(Default): One port block from each NATIP will be allocated and once all the NATIPs are over second port block from each

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			NATIP will be allocated and so on. To understand better if we assume port blocks of all NAT IPs as two dimensional array, PORTS policy follows "row major order" and IPADDRS policy follows "column major order" while allocating port blocks. Example: Client IPs: 2.2.2.1, 2.2.2.2 and 2.2.2.3 NAT IPs and PORT Blocks: 4.4.4.1:PB1, PB2, PB3,., PBn 4.4.4.2: PB1, PB2, PB3,., PBn PORTS Policy: 2.2.2.1 => 4.4.4.1:PB1 2.2.2.2 => 4.4.4.1:PB2

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			2.2.2.3 => 4.4.4.1:PB3 IPADDRS Policy: 2.2.2.1 => 4.4.4.1:PB1 2.2.2.2 => 4.4.4.2:PB1 2.2.2.3 => 4.4.4.1:PB2. Default value: PORTS Possible values = PORTS, IPADDRS
portblocksize	<Integer>	Read-write	Size of the NAT port block to be allocated for each subscriber. To set this parameter for Dynamic NAT, you must enable the port block allocation parameter in the bound LSN pool. For Deterministic NAT, the port block allocation parameter is always enabled, and you cannot disable it.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			In Dynamic NAT, the Citrix ADC allocates a random NAT port block, from the available NAT port pool of an NAT IP address, for each subscriber. For a subscriber, if all the ports are allocated from the subscriber's allocated port block, the ADC allocates a new random port block for the subscriber. The default port block size is 256 for Deterministic NAT, and 0 for Dynamic NAT. Default value: 0 Minimum value = 256 Maximum value = 65536
logging	<String>	Read-write	Log mapping entries and sessions created or deleted for this LSN group. The Citrix ADC logs LSN sessions for this LSN group only when

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			both logging and session logging parameters are enabled. The ADC uses its existing syslog and audit log framework to log LSN information. You must enable global level LSN logging by enabling the LSN parameter in the related NSLOG action and SYLOG action entities. When the Logging parameter is enabled, the Citrix ADC generates log messages related to LSN mappings and LSN sessions of this LSN group. The ADC then sends these log messages to servers associated with the NSLOG action and SYSLOG actions entities. A log message for an LSN mapping entry consists of the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			following information: * NSIP address of the Citrix ADC * Time stamp * Entry type (MAPPING or SESSION) * Whether the LSN mapping entry is created or deleted * Subscriber's IP address, port, and traffic domain ID * NAT IP address and port * Protocol name * Destination IP address, port, and traffic domain ID might be present, depending on the following conditions: ** Destination IP address and port are not logged for Endpoint-Independent mapping

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			** Only Destination IP address (and not port) is logged for Address-Dependent mapping ** Destination IP address and port are logged for Address-Port-Dependent mapping. Default value: DISABLED Possible values = ENABLED, DISABLED
sessionlogging	<String>	Read-write	Log sessions created or deleted for the LSN group. The Citrix ADC logs LSN sessions for this LSN group only when both logging and session logging parameters are enabled. A log message for an LSN session consists of the following information: * NSIP address of the Citrix ADC

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			* Time stamp * Entry type (MAPPING or SESSION) * Whether the LSN session is created or removed * Subscriber's IP address, port, and traffic domain ID * NAT IP address and port * Protocol name * Destination IP address, port, and traffic domain ID. Default value: DISABLED Possible values = ENABLED, DISABLED
sessionsync	<String>	Read-write	In a high availability (HA) deployment, synchronize information of all LSN sessions related to this LSN group with the secondary node. After a failover, established TCP connections and UDP packet flows

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			are kept active and resumed on the secondary node (new primary). For this setting to work, you must enable the global session synchronization parameter. Default value: ENABLED Possible values = ENABLED, DISABLED
snmptraplimit	<Integer>	Read-write	Maximum number of SNMP Trap messages that can be generated for the LSN group in one minute. Default value: 100 Minimum value = 0 Maximum value = 10000
ftp	<String>	Read-write	Enable Application Layer Gateway (ALG) for the FTP protocol. For some application-layer protocols, the IP addresses and protocol port numbers are usually

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			communicated in the packet's payload. When acting as an ALG, the Citrix ADC changes the packet's payload to ensure that the protocol continues to work over LSN. Note: The Citrix ADC also includes ALG for ICMP and TFTP protocols. ALG for the ICMP protocol is enabled by default, and there is no provision to disable it. ALG for the TFTP protocol is disabled by default. ALG is enabled automatically for an LSN group when you bind a UDP LSN application profile, with endpoint-independent-mapping, endpoint-independent filtering, and destination port as 69 (well-known port for TFTP), to the LSN group.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: ENABLED Possible values = ENABLED, DISABLED
pptp	<String>	Read-write	Enable the PPTP Application Layer Gateway. Default value: DISABLED Possible values = ENABLED, DISABLED
sipalg	<String>	Read-write	Enable the SIP ALG. Default value: DISABLED Possible values = ENABLED, DISABLED
rtspalg	<String>	Read-write	Enable the RTSP ALG. Default value: DISABLED Possible values = ENABLED, DISABLED
ip6profile	<String>	Read-write	Name of the LSN ip6 profile to associate with the specified LSN group. An ip6 profile can be associated with a

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			group only during group creation. By default, no LSN ip6 profile is associated with an LSN group during its creation. Only one ip6profile can be associated with a group. Minimum length = 1 Maximum length = 127
ftpcm	<String>	Read-write	Enable the FTP connection mirroring for specified LSN group. Connection mirroring (CM or connection failover) refers to keeping active an established TCP or UDP connection when a failover occurs. Default value: DISABLED Possible values = ENABLED, DISABLED
groupid	<Integer>	Read-only	. Minimum value = 1
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsngroup **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"lsngroup":{

<b>"groupname":<String_value>,

</b><b>"clientname":<String_value>,

</b>"nattype":<String_value>,

"allocpolicy":<String_value>,

"portblocksize":<Integer_value>,

"logging":<String_value>,

"sessionlogging":<String_value>,

"sessionsync":<String_value>,

"snmptraplimit":<Integer_value>,

"ftp":<String_value>,

"pptp":<String_value>,

"sipalg":<String_value>,

"rtspalg":<String_value>,

"ip6profile":<String_value>,

"ftpcm":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsngroup/ groupname_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsngroup **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"lsngroup":{

<b>"groupname":<String_value>,

</b>"portblocksize":<Integer_value>,

"logging":<String_value>,

"sessionlogging":<String_value>,

"sessionsync":<String_value>,

"snmptraplimit":<Integer_value>,

"ftp":<String_value>,
```

```
"pptp":<String_value>,

"sipalg":<String_value>,

"rtspalg":<String_value>,

"ftpcm":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsngroup? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"lsngroup":{

<b>"groupname":<String_value>,

</b>"portblocksize":true,

"logging":true,

"sessionlogging":true,

"sessionsync":true,

"snmptraplimit":true,

"ftp":true,
```

```
"pptp":true,

"sipalg":true,

"rtspalg":true,

"ftpcm":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsngroup **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/lsngroup? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/lsngroup? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of lsngroup resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/lsngroup? **view=summary**

Use this query-parameter to get the summary output of lsngroup resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/lsngroup? **pagesize=#no;pageno=#no**

Use this query-parameter to get the lsngroup resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "lsngroup": [ {

"groupname":<String_value>,

"clientname":<String_value>,

"nattype":<String_value>,

"allocpolicy":<String_value>,

"portblocksize":<Integer_value>,

"logging":<String_value>,

"sessionlogging":<String_value>,

"sessionsync":<String_value>,

"snmptraplimit":<Integer_value>,

"ftp":<String_value>,

"pptp":<String_value>,

"groupid":<Integer_value>,

"sipalg":<String_value>,

"rtspalg":<String_value>,
```

```
"ip6profile":<String_value>,

"ftpcm":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsngroup/ groupname_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/lsngroup/ groupname_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/lsngroup/ groupname_value<String> ? **view=summary**

Use this query-parameter to get the summary output of lsngroup resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lsngroup": [ {

"groupname":<String_value>,

"clientname":<String_value>,

"nattype":<String_value>,

"allocpolicy":<String_value>,

"portblocksize":<Integer_value>,

"logging":<String_value>,

"sessionlogging":<String_value>,

"sessionsync":<String_value>,

"snmptraplimit":<Integer_value>,

"ftp":<String_value>,

"pptp":<String_value>,

"groupid":<Integer_value>,

"sipalg":<String_value>,

"rtspalg":<String_value>,

"ip6profile":<String_value>,

"ftpcm":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsngroup? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "lsngroup": [ { "__count": "#no"} ] }
```

lsngroup_binding

Binding object which returns the resources bound to lsngroup.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
groupname	<String>	Read-write	Name for the LSN group. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			be changed after the LSN group is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "lsn group1" or 'lsn group1'). Minimum length = 1 Maximum length = 127
lsngroup_ipsecalgprofile_binding	<lsngroup_ipsecalgprofile_binding[]>	Read-only	ipsecalgprofile that can be bound to lsngroup.
lsngroup_lsnappsprofile_binding	<lsngroup_lsnappsprofile_binding[]>	Read-only	lsnappsprofile that can be bound to lsngroup.
lsngroup_pcpserver_binding	<lsngroup_pcpserver_binding[]>	Read-only	pcpserver that can be bound to lsngroup.
lsngroup_lsntransportprofile_binding	<lsngroup_lsntransportprofile_binding[]>	Read-only	lsntransportprofile that can be bound to lsngroup.
lsngroup_lsnsipalgprofile_binding	<lsngroup_lsnsipalgprofile_binding[]>	Read-only	lsnsipalgprofile that can be bound to lsngroup.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
lsngroup_lsnlogprofile_binding	<lsngroup_lsnlogprofile_binding[]>	Read-only	lsnlogprofile that can be bound to lsngroup.
lsngroup_lsnpool_binding	<lsngroup_lsnpool_binding[]>	Read-only	lsnpool that can be bound to lsngroup.
lsngroup_lsnrtspalgprofile_binding	<lsngroup_lsnrtspalgprofile_binding[]>	Read-only	lsnrtspalgprofile that can be bound to lsngroup.
lsngroup_lsnhttphdrlogprofile_binding	<lsngroup_lsnhttphdrlogprofile_binding[]>	Read-only	lsnhttphdrlogprofile that can be bound to lsngroup.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsngroup_binding/ groupname_value<String>
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "lsngroup_binding": [ {

"groupname":<String_value>,

"lsngroup_lsnsipalgprofile_binding":<lsngroup_lsnsipalgprofile_binding[]_v
alue>,

"lsngroup_lsnhttphdrlogprofile_binding":<lsngroup_lsnhttphdrlogprofile_bin
ding[]_value>,

"lsngroup_lsnlogprofile_binding":<lsngroup_lsnlogprofile_binding[]_value>,

"lsngroup_lsnpool_binding":<lsngroup_lsnpool_binding[]_value>,

"lsngroup_lsnrtspalgprofile_binding":<lsngroup_lsnrtspalgprofile_binding[]
_value>,
```

```
"lsngroup_lsntransportprofile_binding":<lsngroup_lsntransportprofile_binding[]_value>,

"lsngroup_pcpserver_binding":<lsngroup_pcpserver_binding[]_value>,

"lsngroup_ipsecalgprofile_binding":<lsngroup_ipsecalgprofile_binding[]_value>,

"lsngroup_lsnappsprofile_binding":<lsngroup_lsnappsprofile_binding[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsngroup_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/lsngroup_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "lsngroup_binding": [ {

"groupname":<String_value>,

"lsngroup_lsnsipalgprofile_binding":<lsngroup_lsnsipalgprofile_binding[]_value>,

"lsngroup_lsnhttphdrlogprofile_binding":<lsngroup_lsnhttphdrlogprofile_binding[]_value>,

"lsngroup_lsnlogprofile_binding":<lsngroup_lsnlogprofile_binding[]_value>,

"lsngroup_lsnpool_binding":<lsngroup_lsnpool_binding[]_value>,

"lsngroup_lsnrtspalgprofile_binding":<lsngroup_lsnrtspalgprofile_binding[]_value>,

"lsngroup_lsntransportprofile_binding":<lsngroup_lsntransportprofile_binding[]_value>,

"lsngroup_pcpserver_binding":<lsngroup_pcpserver_binding[]_value>,

"lsngroup_ipsecalgprofile_binding":<lsngroup_ipsecalgprofile_binding[]_value>,

"lsngroup_lsnappsprofile_binding":<lsngroup_lsnappsprofile_binding[]_value>

}]}
```

lsngroup_ipsecalgprofile_binding

Binding object showing the ipsecalgprofile that can be bound to lsngroup.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
groupname	<String>	Read-write	Name for the LSN group. Must begin with an ASCII

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the LSN group is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "lsn group1" or 'lsn group1'). Minimum length = 1 Maximum length = 127
ipsecalgprofile	<String>	Read-write	Name of the IPSec ALG profile to bind to the specified LSN group.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/lsngroup_ipsecalgprofile_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"lsngroup_ipsecalgprofile_binding":{

<b>"groupname":<String_value>,

</b>"ipsecalgprofile":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsngroup_ipsecalgprofile_binding/ groupname_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ lsngroup_ipsecalgprofile_binding/ groupname_value<String> ? **args=ipsecalgprofile: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsngroup_ipsecalgprofile_binding/ groupname_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ lsngroup_ipsecalgprofile_binding/ groupname_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of lsngroup_ipsecalgprofile_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/lsngroup_ipsecalgprofile_binding/ groupname_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the lsngroup_ipsecalgprofile_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lsngroup_ipsecalgprofile_binding": [ {

"groupname":<String_value>,

"ipsecalgprofile":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsngroup_ipsecalgprofile_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/lsngroup_ipsecalgprofile_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lsngroup_ipsecalgprofile_binding": [ {

"groupname":<String_value>,

"ipsecalgprofile":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsngroup_ipsecalgprofile_binding/groupname_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"lsngroup_ipsecalgprofile_binding": [ { "__count": "#no"} ] }
```

lsngroup_lsnappsprofile_binding

Binding object showing the lsnappsprofile that can be bound to lsngroup.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
groupname	<String>	Read-write	Name for the LSN group. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the LSN group is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			quotation marks (for example, "lsn group1" or 'lsn group1'). Minimum length = 1 Maximum length = 127
appsprofilename	<String>	Read-write	Name of the LSN application profile to bind to the specified LSN group. For each set of destination ports, bind a profile for each protocol for which you want to specify settings.

By default, one LSN application profile with default settings for TCP, UDP, and ICMP protocols for all destination ports is bound to an LSN group during its creation. This profile is called a default application profile.

When you bind an LSN application profile, with a specified set of destination ports, to an LSN group, the bound profile overrides the default LSN application profile for that protocol at that set of destination ports.

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/lsngroup_lsnappsprofile_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"lsngroup_lsnappsprofile_binding":{

<b>"groupname":<String_value>,
```

```
</b>"appsprofilename":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsngroup_lsnappsprofile_binding/ groupname_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ lsngroup_lsnappsprofile_binding/ groupname_value<String> ? **args=appsprofilename: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsngroup_lsnappsprofile_binding/ groupname_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ lsngroup_lsnappsprofile_binding/ groupname_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of lsngroup_lsnappsprofile_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/lsngroup_lsnappsprofile_binding/ groupname_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the lsngroup_lsnappsprofile_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lsngroup_lsnappsprofile_binding": [ {

"groupname":<String_value>,

"appsprofilename":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsngroup_lsnappsprofile_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/lsngroup_lsnappsprofile_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lsngroup_lsnappsprofile_binding": [ {

"groupname":<String_value>,

"appsprofilename":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsngroup_lsnappsprofile_binding/ groupname_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"lsngroup_lsnappsprofile_binding": [ { "__count": "#no"} ] }
```

lsngroup_lsnhttphdrlogprofile_binding

Binding object showing the lsnhttphdrlogprofile that can be bound to lsngroup.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
httphdrlogprofilename	<String>	Read-write	The name of the LSN HTTP header logging Profile.
groupname	<String>	Read-write	Name for the LSN group. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the LSN group is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "lsn group1" or 'lsn group1').

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum length = 1 Maximum length = 127
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/lsngroup_lsnhttphdrlogprofile_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"lsngroup_lsnhttphdrlogprofile_binding":{

<b>"groupname":<String_value>,

</b>"httphdrlogprofilename":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsngroup_lsnhttphdrlogprofile_binding/ groupname_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ lsngroup_lsnhttphdrlogprofile_binding/ groupname_value<String> ? **args=httphdrlogprofilename: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsngroup_lsnhttphdrlogprofile_binding/ groupname_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ lsngroup_lsnhttphdrlogprofile_binding/ groupname_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of lsngroup_lsnhttphdrlogprofile_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/lsngroup_lsnhttphdrlogprofile_binding/ groupname_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the lsngroup_lsnhttphdrlogprofile_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lsngroup_lsnhttphdrlogprofile_binding": [ {

"httphdrlogprofilename":<String_value>,

"groupname":<String_value>
```

```
}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsngroup_lsnhttphdrlogprofile_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/lsngroup_lsnhttphdrlogprofile_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lsngroup_lsnhttphdrlogprofile_binding": [ {

"httphdrlogprofilename":<String_value>,

"groupname":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsngroup_lsnhttphdrlogprofile_binding/ groupname_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"lsngroup_lsnhttphdrlogprofile_binding": [ { "__count": "#no"} ] }
```

lsngroup_lsnlogprofile_binding

Binding object showing the lsnlogprofile that can be bound to lsngroup.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
groupname	<String>	Read-write	Name for the LSN group. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the LSN group is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "lsn group1" or 'lsn group1'). Minimum length = 1 Maximum length = 127
logprofilename	<String>	Read-write	The name of the LSN logging Profile.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/lsngroup_lsnlogprofile_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"lsngroup_lsnlogprofile_binding":{

<b>"groupname":<String_value>,
```

```
</b>"logprofilename":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsngroup_lsnlogprofile_binding/ groupname_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ lsngroup_lsnlogprofile_binding/ groupname_value<String> ? **args=logprofilename: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsngroup_lsnlogprofile_binding/ groupname_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ lsngroup_lsnlogprofile_binding/ groupname_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of lsngroup_lsnlogprofile_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/lsngroup_lsnlogprofile_binding/ groupname_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the lsngroup_lsnlogprofile_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lsngroup_lsnlogprofile_binding": [ {

"groupname":<String_value>,

"logprofilename":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsngroup_lsnlogprofile_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/lsngroup_lsnlogprofile_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lsngroup_lsnlogprofile_binding": [ {

"groupname":<String_value>,

"logprofilename":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsngroup_lsnlogprofile_binding/ groupname_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"lsngroup_lsnlogprofile_binding": [ { "__count": "#no"} ] }
```

lsngroup_lsnpool_binding

Binding object showing the lsnpool that can be bound to lsngroup.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
groupname	<String>	Read-write	Name for the LSN group. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the LSN group is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "lsn group1" or 'lsn group1'). Minimum length = 1 Maximum length = 127

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
poolname	<String>	Read-write	Name of the LSN pool to bind to the specified LSN group. Only LSN Pools and LSN groups with the same NAT type settings can be bound together. Multiples LSN pools can be bound to an LSN group.

For Deterministic NAT, pools bound to an LSN group cannot be bound to other LSN groups. For Dynamic NAT, pools bound to an LSN group can be bound to multiple LSN groups.

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of

creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/lsngroup_lsnpool_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"lsngroup_lsnpool_binding":{

<b>"groupname":<String_value>,

</b>"poolname":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsngroup_lsnpool_binding/ groupname_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ lsngroup_lsnpool_binding/ groupname_value<String> ? **args=poolname: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsngroup_lsnpool_binding/ groupname_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ lsngroup_lsnpool_binding/ groupname_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of lsngroup_lsnpool_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/lsngroup_lsnpool_binding/ groupname_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the lsngroup_lsnpool_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lsngroup_lsnpool_binding": [ {

"groupname":<String_value>,

"poolname":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsngroup_lsnpool_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/lsngroup_lsnpool_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lsngroup_lsnpool_binding": [ {

"groupname":<String_value>,
```

```
"poolname":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsngroup_lsnpool_binding/ groupname_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"lsngroup_lsnpool_binding": [ { "__count": "#no"} ] }
```

lsngroup_lsnrtspalgprofile_binding

Binding object showing the lsnrtspalgprofile that can be bound to lsngroup.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
rtspalgprofilename	<String>	Read-write	The name of the LSN RTSP ALG Profile.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
groupname	<String>	Read-write	Name for the LSN group. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the LSN group is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "lsn group1" or 'lsn group1'). Minimum length = 1 Maximum length = 127
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD

- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/lsngroup_lsnrtspalgprofile_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"lsngroup_lsnrtspalgprofile_binding":{

<b>"groupname":<String_value>,

</b>"rtspalgprofilename":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsngroup_lsnrtspalgprofile_binding/ groupname_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ lsngroup_lsnrtspalgprofile_binding/ groupname_value<String> ? **args=rtspalgprofilename: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsngroup_lsnrtspalgprofile_binding/ groupname_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ lsngroup_lsnrtspalgprofile_binding/ groupname_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of lsngroup_lsnrtspalgprofile_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/lsngroup_lsnrtspalgprofile_binding/groupname_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the lsngroup_lsnrtspalgprofile_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lsngroup_lsnrtspalgprofile_binding": [ {

"rtspalgprofilename":<String_value>,

"groupname":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsngroup_lsnrtspalgprofile_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/lsngroup_lsnrtspalgprofile_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lsngroup_lsnrtspalgprofile_binding": [ {

"rtspalgprofilename":<String_value>,

"groupname":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsngroup_lsnrtspalgprofile_binding/groupname_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"lsngroup_lsnrtspalgprofile_binding": [ { "__count": "#no"} ] }
```

lsngroup_lsnsipalgprofile_binding

Binding object showing the lsnsipalgprofile that can be bound to lsngroup.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
groupname	<String>	Read-write	Name for the LSN group. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the LSN group is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			quotation marks (for example, "lsn group1" or 'lsn group1'). Minimum length = 1 Maximum length = 127
sipalgprofilename	<String>	Read-write	The name of the LSN SIP ALG Profile.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/lsngroup_lsnsipalgprofile_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"lsngroup_lsnsipalgprofile_binding":{

<b>"groupname":<String_value>,

</b>"sipalgprofilename":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsngroup_lsnsipalgprofile_binding/ groupname_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ lsngroup_lsnsipalgprofile_binding/ groupname_value<String> ? **args=sipalgprofilename: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsngroup_lsnsipalgprofile_binding/ groupname_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ lsngroup_lsnsipalgprofile_binding/ groupname_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of lsngroup_lsnsipalgprofile_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/lsngroup_lsnsipalgprofile_binding/ groupname_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the lsngroup_lsnsipalgprofile_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lsngroup_lsnsipalgprofile_binding": [ {

"groupname":<String_value>,

"sipalgprofilename":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsngroup_lsnsipalgprofile_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/lsngroup_lsnsipalgprofile_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lsngroup_lsnsipalgprofile_binding": [ {

"groupname":<String_value>,

"sipalgprofilename":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsngroup_lsnsipalgprofile_binding/groupname_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"lsngroup_lsnsipalgprofile_binding": [ { "__count": "#no"} ] }
```

lsngroup_lsntransportprofile_binding

Binding object showing the lsntransportprofile that can be bound to lsngroup.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
transportprofilename	<String>	Read-write	Name of the LSN transport profile to bind to the specified LSN group. Bind a profile for each protocol for which you want to specify settings.

By default, one LSN transport profile with default settings for TCP, UDP, and ICMP protocols is bound to an LSN group during its creation. This profile is called a default transport.

An LSN transport profile that you bind to an LSN group overrides the default LSN transport profile for that protocol.

Minimum length = 1

Maximum length = 127

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/lsngroup_lsntransportprofile_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"lsngroup_lsntransportprofile_binding":{

<b>"groupname":<String_value>,

</b>"transportprofilename":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsngroup_lsntransportprofile_binding/ groupname_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ lsngroup_lsntransportprofile_binding/ groupname_value<String> ? **args=transportprofilename: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsngroup_lsntransportprofile_binding/ groupname_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ lsngroup_lsntransportprofile_binding/ groupname_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of lsngroup_lsntransportprofile_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/lsngroup_lsntransportprofile_binding/ groupname_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the lsngroup_lsntransportprofile_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lsngroup_lsntransportprofile_binding": [ {

"transportprofilename":<String_value>,

"groupname":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsngroup_lsntransportprofile_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/lsngroup_lsntransportprofile_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lsngroup_lsntransportprofile_binding": [ {

"transportprofilename":<String_value>,

"groupname":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsngroup_lsntransportprofile_binding/ groupname_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"lsngroup_lsntransportprofile_binding": [ { "__count": "#no"} ] }
```

lsngroup_pcpserver_binding

Binding object showing the pcpserver that can be bound to lsngroup.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
pcpserver	<String>	Read-write	Name of the PCP server to be associated with lsn group.
groupname	<String>	Read-write	Name for the LSN group. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the LSN group is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "lsn group1" or 'lsn group1'). Minimum length = 1 Maximum length = 127
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/lsngroup_pcpserver_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"lsngroup_pcpserver_binding":{

<b>"groupname":<String_value>,

</b>"pcpserver":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsngroup_pcpserver_binding/ groupname_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ lsngroup_pcpserver_binding/ groupname_value<String> ? **args=pcpserver: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsngroup_pcpserver_binding/ groupname_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/

lsngroup_pcpserver_binding/ groupname_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of lsngroup_pcpserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/lsngroup_pcpserver_binding/ groupname_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the lsngroup_pcpserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lsngroup_pcpserver_binding": [ {

"pcpserver":<String_value>,

"groupname":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsngroup_pcpserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/lsngroup_pcpserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lsngroup_pcpserver_binding": [ {

"pcpserver":<String_value>,

"groupname":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsngroup_pcpserver_binding/groupname_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"lsngroup_pcpserver_binding": [ { "__count": "#no"} ] }
```

lsnhttphdrlogprofile

Configuration for LSN HTTP header logging Profile resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
httphdrlogprofilename	<String>	Read-write	The name of the HTTP header logging Profile. Minimum length = 1 Maximum length = 127
logurl	<String>	Read-write	URL information is logged if option is enabled. Default value: ENABLED Possible values = ENABLED, DISABLED
logmethod	<String>	Read-write	HTTP method information is logged if option is enabled.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: ENABLED Possible values = ENABLED, DISABLED
logversion	<String>	Read-write	Version information is logged if option is enabled. Default value: ENABLED Possible values = ENABLED, DISABLED
loghost	<String>	Read-write	Host information is logged if option is enabled. Default value: ENABLED Possible values = ENABLED, DISABLED
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET

- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnhttphdrlogprofile **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"lsnhttphdrlogprofile":{

<b>"httphdrlogprofilename":<String_value>,

</b>"logurl":<String_value>,

"logmethod":<String_value>,

"logversion":<String_value>,

"loghost":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnhttphdrlogprofile/ httphdrlogprofilename_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnhttphdrlogprofile **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"lsnhttphdrlogprofile":{

<b>"httphdrlogprofilename":<String_value>,

</b>"logurl":<String_value>,

"logmethod":<String_value>,

"logversion":<String_value>,

"loghost":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnhttphdrlogprofile? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"lsnhttphdrlogprofile":{

<b>"httphdrlogprofilename":<String_value>,

</b>"logurl":true,

"logmethod":true,

"logversion":true,

"loghost":true
```

```
}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnhttphdrlogprofile **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/lsnhttphdrlogprofile? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/lsnhttphdrlogprofile? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of lsnhttphdrlogprofile resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/lsnhttphdrlogprofile? **view=summary**

Use this query-parameter to get the summary output of lsnhttphdrlogprofile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/lsnhttphdrlogprofile? **pagesize=#no;pageno=#no**

Use this query-parameter to get the lsnhttphdrlogprofile resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "lsnhttphdrlogprofile": [ {

"httphdrlogprofilename":<String_value>,

"logurl":<String_value>,

"logmethod":<String_value>,

"logversion":<String_value>,

"loghost":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnhttphdrlogprofile/ httphdrlogprofilename_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> / nitro/v1/config/lsnhttphdrlogprofile/ httphdrlogprofilename_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/lsnhttphdrlogprofile/ httphdrlogprofilename_value<String> ? **view=summary**

Use this query-parameter to get the summary output of lsnhttphdrlogprofile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lsnhttphdrlogprofile": [ {

"httphdrlogprofilename":<String_value>,

"logurl":<String_value>,

"logmethod":<String_value>,

"logversion":<String_value>,

"loghost":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnhttphdrlogprofile? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "lsnhttphdrlogprofile": [ { "__count": "#no"} ] }
```

lsnip6profile

Configuration for LSN ip6 Profile resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the LSN ip6 profile. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the LSN ip6 profile is created. The following requirement applies only to the Citrix

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "lsn ip6 profile1" or 'lsn ip6 profile1'). Minimum length = 1 Maximum length = 127
type	<String>	Read-write	IPv6 translation type for which to set the LSN IP6 profile parameters. Possible values = DS-Lite, NAT64
natprefix	<String>	Read-write	IPv6 address(es) of the LSN subscriber(s) or subscriber network(s) on whose traffic you want the Citrix ADC to perform Large Scale NAT.
network6	<String>	Read-write	IPv6 address of the Citrix ADC AFTR device.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnip6profile **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"lsnip6profile":{

<b>"name":<String_value>,

</b><b>"type":<String_value>,

</b>"natprefix":<String_value>,

"network6":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnip6profile/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnip6profile **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/lsnip6profile? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/lsnip6profile? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of lsnip6profile resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/lsnip6profile? **view=summary**

Use this query-parameter to get the summary output of lsnip6profile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/lsnip6profile? **pagesize=#no;pageno=#no**

Use this query-parameter to get the lsnip6profile resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "lsnip6profile": [ {

"name":<String_value>,

"type":<String_value>,

"network6":<String_value>,

"natprefix":<String_value>,

"_nextgenapiresource":<String_value>
```

```
}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnip6profile/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/lsnip6profile/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/lsnip6profile/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of lsnip6profile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lsnip6profile": [ {

"name":<String_value>,

"type":<String_value>,
```

```
"network6":<String_value>,

"natprefix":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnip6profile? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "lsnip6profile": [ { "__count": "#no"} ] }
```

lsnlogprofile

Configuration for LSN logging Profile resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
logprofilename	<String>	Read-write	The name of the logging Profile. Minimum length = 1 Maximum length = 127
logsubscrinfo	<String>	Read-write	Subscriber ID information is logged if option is enabled. Default value: DISABLED Possible values = ENABLED, DISABLED
logcompact	<String>	Read-write	Logs in Compact Logging format if option is enabled. Default value: ENABLED Possible values = ENABLED, DISABLED
logipfix	<String>	Read-write	Logs in IPFIX format if option is enabled. Default value: DISABLED Possible values = ENABLED, DISABLED
analyticsprofile	<String>	Read-write	Name of the Analytics Profile

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			attached to this lsn profile.
logsessdeletion	<String>	Read-write	LSN Session deletion will not be logged if disabled. Default value: ENABLED Possible values = ENABLED, DISABLED
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnlogprofile **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"lsnlogprofile":{

<b>"logprofilename":<String_value>,

</b>"logsubscrinfo":<String_value>,

"logcompact":<String_value>,

"logipfix":<String_value>,

"analyticsprofile":<String_value>,

"logsessdeletion":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnlogprofile/ logprofilename_value<String>
HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnlogprofile **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"lsnlogprofile":{

<b>"logprofilename":<String_value>,

</b>"logsubscrinfo":<String_value>,

"logcompact":<String_value>,

"logipfix":<String_value>,

"analyticsprofile":<String_value>,

"logsessdeletion":<String_value>
```

```
}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnlogprofile? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"lsnlogprofile":{

<b>"logprofilename":<String_value>,

</b>"logsubscrinfo":true,

"logcompact":true,

"logipfix":true,

"analyticsprofile":true,

"logsessdeletion":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnlogprofile **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/lsnlogprofile? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/lsnlogprofile? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of lsnlogprofile resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/lsnlogprofile? **view=summary**

Use this query-parameter to get the summary output of lsnlogprofile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/lsnlogprofile? **pagesize=#no;pageno=#no**

Use this query-parameter to get the lsnlogprofile resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "lsnlogprofile": [ {

"logprofilename":<String_value>,

"logsubscrinfo":<String_value>,

"logcompact":<String_value>,

"logipfix":<String_value>,

"analyticsprofile":<String_value>,

"logsessdeletion":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnlogprofile/ logprofilename_value<String>
Query-parameters: attrs http:// <netscaler-ip-address> /nitro/v1/config/lsnlogprofile/ logprofilename_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/lsnlogprofile/ logprofilename_value<String> ? **view=summary**

Use this query-parameter to get the summary output of lsnlogprofile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lsnlogprofile": [ {

"logprofilename":<String_value>,

"logsubscrinfo":<String_value>,

"logcompact":<String_value>,

"logipfix":<String_value>,

"analyticsprofile":<String_value>,

"logsessdeletion":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnlogprofile? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "lsnlogprofile": [ { "__count": "#no"} ] }
```

lsnparameter

Configuration for LSN parameter resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
memlimit	<Integer>	Read-write	Amount of Citrix ADC memory to reserve for the LSN feature, in multiples of 2MB. Note: If you later reduce the value of this parameter, the amount of active memory is not reduced. Changing the configured memory limit can only increase the amount of active memory. This command is deprecated, use 'set extendedmemoryparam -memlimit' instead.
sessionsync	<String>	Read-write	Synchronize all LSN sessions with the secondary node in a

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			high availability (HA) deployment (global synchronization). After a failover, established TCP connections and UDP packet flows are kept active and resumed on the secondary node (new primary). The global session synchronization parameter and session synchronization parameters (group level) of all LSN groups are enabled by default. For a group, when both the global level and the group level LSN session synchronization parameters are enabled, the primary node synchronizes information of all LSN sessions related to this LSN group with the secondary node.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: ENABLED Possible values = ENABLED, DISABLED
subscrsessionremoval	<String>	Read-write	LSN global setting for controlling subscriber aware session removal, when this is enabled, when ever the subscriber info is deleted from subscriber database, sessions corresponding to that subscriber will be removed. if this setting is disabled, subscriber sessions will be timed out as per the idle time out settings. Default value: DISABLED Possible values = ENABLED, DISABLED
memlimitactive	<Integer>	Read-only	Amount of actual memory reserved for the LSN feature. The amount of active memory for the LSN feature might be less than the configured

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			memory, because the available memory is shared across features.
maxmemlimit	<Integer>	Read-only	Maximum amount of Citrix ADC memory that can be reserved for the LSN feature.
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- UPDATE
- UNSET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnparameter **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"lsnparameter":{

"memlimit":<Integer_value>,

"sessionsync":<String_value>,

"subscrsessionremoval":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnparameter? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"lsnparameter":{

"memlimit":true,

"sessionsync":true,

"subscrsessionremoval":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnparameter **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "lsnparameter": [ {

"memlimitactive":<Integer_value>,

"maxmemlimit":<Integer_value>,
```

```
"memlimit":<Integer_value>,

"sessionsync":<String_value>,

"subscrsessionremoval":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

lsnpool

Configuration for LSN pool resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
poolname	<String>	Read-write	Name for the LSN pool. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the LSN pool is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			enclose the name in double or single quotation marks (for example, "lsn pool1" or 'lsn pool1'). Minimum length = 1 Maximum length = 127
nattype	<String>	Read-write	Type of NAT IP address and port allocation (from the LSN pools bound to an LSN group) for subscribers (of the LSN client entity bound to the LSN group): Available options function as follows: * Deterministic - Allocate a NAT IP address and a block of ports to each subscriber (of the LSN client bound to the LSN group). The Citrix ADC sequentially allocates NAT resources to these subscribers. The Citrix ADC ADC assigns the first block of ports (block size determined by the port block size

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			parameter of the LSN group) on the beginning NAT IP address to the beginning subscriber IP address. The next range of ports is assigned to the next subscriber, and so on, until the NAT address does not have enough ports for the next subscriber. In this case, the first port block on the next NAT address is used for the subscriber, and so on. Because each subscriber now receives a deterministic NAT IP address and a block of ports, a subscriber can be identified without any need for logging. For a connection, a subscriber can be identified based only on the NAT IP address and port,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			and the destination IP address and port. * Dynamic - Allocate a random NAT IP address and a port from the LSN NAT pool for a subscriber's connection. If port block allocation is enabled (in LSN pool) and a port block size is specified (in the LSN group), the Citrix ADC allocates a random NAT IP address and a block of ports for a subscriber when it initiates a connection for the first time. The ADC allocates this NAT IP address and a port (from the allocated block of ports) for different connections from this subscriber. If all the ports are allocated (for different subscriber's connections) from

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			the subscriber's allocated port block, the ADC allocates a new random port block for the subscriber. Only LSN Pools and LSN groups with the same NAT type settings can be bound together. Multiples LSN pools can be bound to an LSN group. A maximum of 16 LSN pools can be bound to an LSN group. . Default value: DYNAMIC Possible values = DYNAMIC, DETERMINISTIC
portblockallocation	<String>	Read-write	Allocate a random NAT port block, from the available NAT port pool of an NAT IP address, for each subscriber when the NAT allocation is set as Dynamic NAT. For any connection initiated from a subscriber, the Citrix ADC allocates a NAT

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			port from the subscriber's allocated NAT port block to create the LSN session. You must set the port block size in the bound LSN group. For a subscriber, if all the ports are allocated from the subscriber's allocated port block, the Citrix ADC allocates a new random port block for the subscriber. For Deterministic NAT, this parameter is enabled by default, and you cannot disable it. Default value: DISABLED Possible values = ENABLED, DISABLED
portrealloctimeout	<Integer>	Read-write	The waiting time, in seconds, between deallocating LSN NAT ports (when an LSN mapping is removed) and reallocating them for

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			a new LSN session. This parameter is necessary in order to prevent collisions between old and new mappings and sessions. It ensures that all established sessions are broken instead of redirected to a different subscriber. This is not applicable for ports used in: * Deterministic NAT * Address-Dependent filtering and Address-Port-Dependent filtering * Dynamic NAT with port block allocation In these cases, ports are immediately reallocated. Default value: 0 Minimum value = 0 Maximum value = 600
maxportrealloctmq	<Integer>	Read-write	Maximum number of ports for which the port reallocation timeout applies for each NAT IP

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			address. In other words, the maximum deallocated-port queue size for which the reallocation timeout applies for each NAT IP address. When the queue size is full, the next port deallocated is reallocated immediately for a new LSN session. Default value: 65536 Minimum value = 0 Maximum value = 65536
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnpool **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"lsnpool":{

<b>"poolname":<String_value>,

</b>"nattype":<String_value>,
```

```
"portblockallocation":<String_value>,

"portrealloctimeout":<Integer_value>,

"maxportrealloctmq":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnpool/ poolname_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnpool **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"lsnpool":{

<b>"poolname":<String_value>,

</b>"portrealloctimeout":<Integer_value>,
```

```
"maxportrealloctmq":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnpool? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"lsnpool":{

<b>"poolname":<String_value>,

</b>"portrealloctimeout":true,

"maxportrealloctmq":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnpool **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/lsnpool? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/lsnpool? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of lsnpool resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/lsnpool? **view=summary**

Use this query-parameter to get the summary output of lsnpool resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/lsnpool? **pagesize=#no;pageno=#no**

Use this query-parameter to get the lsnpool resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "lsnpool": [ {

"poolname":<String_value>,

"nattype":<String_value>,

"portrealloctimeout":<Integer_value>,

"maxportrealloctmq":<Integer_value>,
```

```
"portblockallocation":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnpool/ poolname_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/lsnpool/ poolname_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/lsnpool/ poolname_value<String> ? **view=summary**

Use this query-parameter to get the summary output of lsnpool resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lsnpool": [ {

"poolname":<String_value>,
```

```
"nattype":<String_value>,

"portrealloctimeout":<Integer_value>,

"maxportrealloctmq":<Integer_value>,

"portblockallocation":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnpool? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "lsnpool": [ { "__count": "#no"} ] }
```

lsnpool_binding

Binding object which returns the resources bound to lsnpool.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
poolname	<String>	Read-write	Name for the LSN pool. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the LSN pool is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "lsn pool1" or 'lsn pool1'). Minimum length = 1 Maximum length = 127
lsnpool_lsnip_binding	<lsnpool_lsnip_binding[]>	Read-only	lsnip that can be bound to lsnpool.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnpool_binding/ poolname_value<String>
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "lsnpool_binding": [ {

"poolname":<String_value>,

"lsnpool_lsnip_binding":<lsnpool_lsnip_binding[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnpool_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/lsnpool_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "lsnpool_binding": [ {

"poolname":<String_value>,
```

```
"lsnpool_lsnip_binding":<lsnpool_lsnip_binding[]_value>

}]}
```

lsnpool_lsnip_binding

Binding object showing the lsnip that can be bound to lsnpool.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
lsnip	<String>	Read-write	IPv4 address or a range of IPv4 addresses to be used as NAT IP address(es) for LSN. After the pool is created, these IPv4 addresses are added to the Citrix ADC as Citrix ADC owned IP address of type LSN. A maximum of 4096 IP addresses can be bound to an LSN pool. An LSN IP address associated with an LSN pool cannot be shared with other LSN pools. IP addresses specified for this parameter must not already exist on the Citrix ADC as any Citrix ADC owned IP addresses. In the command line interface, separate

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			the range with a hyphen. For example: 10.102.29.30-10.102 .29.189. You can later remove some or all the LSN IP addresses from the pool, and add IP addresses to the LSN pool. By default , arp is enabled on LSN IP address but, you can disable it using command - "set ns ip" . Minimum length = 1
poolname	<String>	Read-write	Name for the LSN pool. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the LSN pool is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			enclose the name in double or single quotation marks (for example, "lsn pool1" or 'lsn pool1'). Minimum length = 1 Maximum length = 127
ownernode	<Integer>	Read-write	ID(s) of cluster node(s) on which command is to be executed. Minimum value = 0 Maximum value = 31
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/lsnpool_lsnip_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"lsnpool_lsnip_binding":{

<b>"poolname":<String_value>,

</b>"ownernode":<Integer_value>,

"lsnip":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnpool_lsnip_binding/ poolname_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ lsnpool_lsnip_binding/ poolname_value<String> ? **args=ownernode: <Integer_value> ,lsnip: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnpool_lsnip_binding/ poolname_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ lsnpool_lsnip_binding/ poolname_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of lsnpool_lsnip_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/lsnpool_lsnip_binding/ poolname_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the lsnpool_lsnip_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lsnpool_lsnip_binding": [ {

"lsnip":<String_value>,

"poolname":<String_value>,

"ownernode":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnpool_lsnip_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/lsnpool_lsnip_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lsnpool_lsnip_binding": [ {

"lsnip":<String_value>,

"poolname":<String_value>,

"ownernode":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnpool_lsnip_binding/ poolname_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"lsnpool_lsnip_binding": [ { "__count": "#no"} ] }
```

lsnrtspalgprofile

Configuration for LSN RTSPALG Profile resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
rtspalgprofilename	<String>	Read-write	The name of the RTSPALG Profile. Minimum length = 1 Maximum length = 127
rtspidletimeout	<Integer>	Read-write	Idle timeout for the rtsp sessions in seconds. Default value: 120
rtspportrange	<String>	Read-write	port for the RTSP.
rtsptransportprotocol	<String>	Read-write	RTSP ALG Profile transport protocol type. Default value: TCP Possible values = TCP, UDP
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- UPDATE
- UNSET

- GET (ALL)
- GET
- COUNT
- DELETE

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnrtspalgprofile **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"lsnrtspalgprofile":{

<b>"rtspalgprofilename":<String_value>,

</b>"rtspidletimeout":<Integer_value>,

<b>"rtspportrange":<String_value>,

</b>"rtsptransportprotocol":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnrtspalgprofile **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"lsnrtspalgprofile":{

<b>"rtspalgprofilename":<String_value>,

</b>"rtspidletimeout":<Integer_value>,

"rtspportrange":<String_value>,

"rtsptransportprotocol":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnrtspalgprofile? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"lsnrtspalgprofile":{

<b>"rtspalgprofilename":<String_value>,

</b>"rtspidletimeout":true,

"rtspportrange":true,

"rtsptransportprotocol":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnrtspalgprofile/ rtspalgprofilename_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnrtspalgprofile **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/lsnrtspalgprofile? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/lsnrtspalgprofile? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of lsnrtspalgprofile resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/lsnrtspalgprofile? **view=summary**

Use this query-parameter to get the summary output of lsnrtspalgprofile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/lsnrtspalgprofile? **pagesize=#no;pageno=#no**

Use this query-parameter to get the lsnrtspalgprofile resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "lsnrtspalgprofile": [ {

"rtspalgprofilename":<String_value>,

"rtspidletimeout":<Integer_value>,

"rtspportrange":<String_value>,

"rtsptransportprotocol":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnrtspalgprofile/ rtspalgprofilename_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/lsnrtspalgprofile/ rtspalgprofilename_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/lsnrtspalgprofile/ rtspalgprofilename_value<String> ? **view=summary**

Use this query-parameter to get the summary output of lsnrtspalgprofile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lsnrtspalgprofile": [ {

"rtspalgprofilename":<String_value>,

"rtspidletimeout":<Integer_value>,

"rtspportrange":<String_value>,

"rtsptransportprotocol":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnrtspalgprofile? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "lsnrtspalgprofile": [ { "__count": "#no"} ] }
```

lsnrtspalgsession

Configuration for LSN RTSPALG session resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
sessionid	<String>	Read-write	Session ID for the RTSP call.
nodeid	<Integer>	Read-write	Unique number that identifies the cluster node. Minimum value = 0 Maximum value = 31
callflags	<Integer>	Read-only	Flags for the call entry.
xlatip	<String>	Read-only	XLAT IP Address if its XLAT session.
callrefcount	<Integer>	Read-only	Reference count for the call entry.
calltimer	<Integer>	Read-only	Timer for the call entry.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET (ALL)
- GET
- COUNT
- FLUSH

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

FLUSH

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnrtspalgsession? **action=flush HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"lsnrtspalgsession":{

<b>"sessionid":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnrtspalgsession **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/lsnrtspalgsession? **args=sessionid: <String_value> ,nodeid: <Integer_value>**

Use this query-parameter to get lsnrtspalgsession resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/config/lsnrtspalgsession? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/lsnrtspalgsession? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of lsnrtspalgsession resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/lsnrtspalgsession? **view=summary**

Use this query-parameter to get the summary output of lsnrtspalgsession resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/lsnrtspalgsession? **pagesize=#no;pageno=#no**

Use this query-parameter to get the lsnrtspalgsession resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "lsnrtspalgsession": [ {

sessionid:<String_value>,nodeid:<Integer_value>"callflags":<Integer_value>
,

"xlatip":<String_value>,

"callrefcount":<Integer_value>,

"calltimer":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnrtspalgsession/ sessionid_value<String>
Query-parameters: attrs http:// <netscaler-ip-address> /nitro/v1/config/lsnrtspalgsession/ sessionid_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/lsnrtspalgsession/ sessionid_value<String> ? **view=summary**

Use this query-parameter to get the summary output of lsnrtspalgsession resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lsnrtspalgsession": [ {

sessionid:<String_value>,nodeid:<Integer_value>"callflags":<Integer_value>
,

"xlatip":<String_value>,

"callrefcount":<Integer_value>,

"calltimer":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnrtspalgsession? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "lsnrtspalgsession": [ { "__count": "#no"} ] }
```

lsnrtspalgsession_binding

Binding object which returns the resources bound to lsnrtspalgsession.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
sessionid	<String>	Read-write	Session ID for the RTSP call.
lsnrtspalgsession_datachannel_binding	<lsnrtspalgsession_datachannel_binding[]>	Read-only	datachannel that can be bound to lsnrtspalgsession.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnrtspalgsession_binding/sessionid_value<String>

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "lsnrtspalgsession_binding": [ {

"sessionid":<String_value>,

"lsnrtspalgsession_datachannel_binding":<lsnrtspalgsession_datachannel_binding[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnrtspalgsession_binding

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters:

bulkbindings

http:// <netscaler-ip-address> /nitro/v1/config/lsnrtspalgsession_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "lsnrtspalgsession_binding": [ {

"sessionid":<String_value>,

"lsnrtspalgsession_datachannel_binding":<lsnrtspalgsession_datachannel_binding[]_value>

}]}
```

lsnrtspalgsession_datachannel_binding

Binding object showing the datachannel that can be bound to lsnrtspalgsession.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
sessionid	<String>	Read-write	Session ID for the RTSP call.
channelip	<String>	Read-write	IP address of the channel.
channelprotocol	<String>	Read-only	Channel transport protocol. Possible values = HTTP, FTP, TCP, UDP, SSL,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			SSL_BRIDGE, SSL_TCP, NNTP, RPCSVR, DNS, ADNS, SNMP, RTSP, DHCPRA, ANY, SIP_UDP, SIP_TCP, SIP_SSL, DNS_TCP, ADNS_TCP, HTTPSVR, HTTPCLIENT, NAT, HA, AAA, SINCTCP, VPN AFTP, MONITORS, SSLVPN UDP, SINCUDP, RIP, UDP CLNT, SASP, RPCCLNTS, ROUTE, AUDIT, STA HTTP, STA SSL, DNS RESOLVE, RDP, MYSQL, MSSQL, DIAMETER, SSL_DIAMETER, TFTP, ORACLE, ICA, RADIUS, RADIUSListener, SMPP, PPTP, GRE, SYSLOGTCP, SYSLOGUDP, FIX, SSL_FIX, QUIC, TFTP_DATA, USER_TCP, USER_SSL_TCP, MONGO,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			MONGO_TLS, MQTT, MQTT_TLS, QUIC_BRIDGE, HTTP_QUIC, CT_TCP, CT_UDP, DOT, ADNS_DOT, ADNS_DOH, KAFKA_BROKER, KAFKA_PRODUCER
channelflags	<Integer>	Read-only	Flags for the call entry.
channelnatport	<Integer>	Read-only	Natted port for the channel.
channeltimeout	<Integer>	Read-only	Timeout for the channel.
channelnatip	<String>	Read-only	Natted IP address of the channel.
channelport	<Integer>	Read-only	port for the channel.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnrtspalgsession_datachannel_binding/ sessionid_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ lsnrtspalgsession_datachannel_binding/ sessionid_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of lsnrtspalgsession_datachannel_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/lsnrtspalgsession_datachannel_binding/ sessionid_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the lsnrtspalgsession_datachannel_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lsnrtspalgsession_datachannel_binding": [ {

"sessionid":<String_value>,

"channelip":<String_value>,

"channelprotocol":<String_value>,

"channelflags":<Integer_value>,

"channelnatport":<Integer_value>,

"channeltimeout":<Integer_value>,

"channelnatip":<String_value>,

"channelport":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnrtspalgsession_datachannel_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/lsnrtspalgsession_datachannel_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lsnrtspalgsession_datachannel_binding": [ {

"sessionid":<String_value>,

"channelip":<String_value>,

"channelprotocol":<String_value>,

"channelflags":<Integer_value>,

"channelnatport":<Integer_value>,

"channeltimeout":<Integer_value>,

"channelnatip":<String_value>,

"channelport":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnrtspalgsession_datachannel_binding/sessionid_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"lsnrtspalgsession_datachannel_binding": [ { "__count": "#no"} ] }
```

lsnsession

Configuration for lsn session resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
nattype	<String>	Read-write	Type of sessions to be displayed. Default value: NAT44 Possible values = NAT44, DS-Lite, NAT64
clientname	<String>	Read-write	Name of the LSN Client entity.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
network	<String>	Read-write	IP address or network address of subscriber(s).
netmask	<String>	Read-write	Subnet mask for the IP address specified by the network parameter.
network6	<String>	Read-write	IPv6 address of the LSN subscriber or B4 device.
td	<Integer>	Read-write	Traffic domain ID of the LSN client entity. Default value: 0 Minimum value = 0 Maximum value = 4094
natip	<String>	Read-write	Mapped NAT IP address used in LSN sessions.
nodeid	<Integer>	Read-write	Unique number that identifies the cluster node. Minimum value = 0 Maximum value = 31
natport2	<Integer>	Read-write	Mapped NAT port used in the LSN sessions.
natprefix	<String>	Read-only	IPv6 address of the LSN subscriber(s) or subscriber

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			network(B4-Device) on whose traffic the Citrix ADC perform Large Scale NAT.
subscrip	<String>	Read-only	The Source IP address.
subscrport	<Integer>	Read-only	The Source Port.
destip	<String>	Read-only	The Destination IP address.
destport	<Integer>	Read-only	The Destination Port.
natport	<Integer>	Read-only	The NAT Port.
transportprotocol	<String>	Read-only	The Transport Protocol for the session. Possible values = TCP, UDP, ICMP
sessionestdir	<String>	Read-only	The Session establishment direction, session was established for outbound or inbound packet. Possible values = OUT, IN
dsttd	<Integer>	Read-only	.
srctd	<Integer>	Read-only	.
ipv6address	<String>	Read-only	IPv6 address of v6 vserver.
_nextgenapiresource	<String>	Read-only	.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET (ALL)
- COUNT
- FLUSH

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

FLUSH

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnsession? **action=flush HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"lsnsession":{

"nattype":<String_value>,

"clientname":<String_value>,

"network":<String_value>,

"netmask":<String_value>,

"network6":<String_value>,

"td":<Integer_value>,

"natip":<String_value>,

"natport2":<Integer_value>,

"nodeid":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnsession **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/lsnsession? **args=nattype: <String_value> ,clientname: <String_value> ,network: <String_value> ,netmask: <String_value> ,network6: <String_value> ,td: <Integer_value> ,natip: <String_value> ,nodeid: <Integer_value>**

Use this query-parameter to get lsnsession resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/config/lsnsession? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/lsnsession? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of lsnsession resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/lsnsession? **view=summary**

Use this query-parameter to get the summary output of lsnsession resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/lsnsession? **pagesize=#no;pageno=#no**

Use this query-parameter to get the lsnsession resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "lsnsession": [ {

nattype:<String_value>,clientname:<String_value>,network:<String_value>,ne
tmask:<String_value>,network6:<String_value>,td:<Integer_value>,natip:<Str
```

```
ing_value>,nodeid:<Integer_value>"natprefix":<String_value>,

"subscrip":<String_value>,

"subscrport":<Integer_value>,

"destip":<String_value>,

"destport":<Integer_value>,

"natport":<Integer_value>,

"transportprotocol":<String_value>,

"sessionestdir":<String_value>,

"dsttd":<Integer_value>,

"srctd":<Integer_value>,

"ipv6address":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnsession? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "lsnsession": [ { "__count": "#no"} ] }
```

lsnsipalgcall

Configuration for LSN SIPALG call resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
callid	<String>	Read-write	Call ID for the SIP call.
nodeid	<Integer>	Read-write	Unique number that identifies the cluster node. Minimum value = 0 Maximum value = 31
callflags	<Integer>	Read-only	Flags for the call entry.
xlatip	<String>	Read-only	XLAT IP Address if its XLAT session.
callrefcount	<Integer>	Read-only	Reference count for the call entry.
calltimer	<Integer>	Read-only	Timer for the call entry.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET (ALL)
- GET
- COUNT
- FLUSH

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

FLUSH

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnsipalgcall? **action=flush HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"lsnsipalgcall":{

<b>"callid":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnsipalgcall **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/lsnsipalgcall? **args=callid: <String_value> ,nodeid: <Integer_value>**

Use this query-parameter to get lsnsipalgcall resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/config/lsnsipalgcall? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/lsnsipalgcall? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of lsnsipalgcall resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/lsnsipalgcall? **view=summary**

Use this query-parameter to get the summary output of lsnsipalgcall resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/lsnsipalgcall? **pagesize=#no;pageno=#no**

Use this query-parameter to get the lsnsipalgcall resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "lsnsipalgcall": [ {

callid:<String_value>,nodeid:<Integer_value>"callflags":<Integer_value>,

"xlatip":<String_value>,

"callrefcount":<Integer_value>,

"calltimer":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnsipalgcall/ callid_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/lsnsipalgcall/ callid_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/lsnsipalgcall/ callid_value<String> ? **view=summary**

Use this query-parameter to get the summary output of lsnsipalgcall resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lsnsipalgcall": [ {

callid:<String_value>,nodeid:<Integer_value>"callflags":<Integer_value>,

"xlatip":<String_value>,

"callrefcount":<Integer_value>,

"calltimer":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnsipalgcall? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "lsnsipalgcall": [ { "__count": "#no"} ] }
```

lsnsipalgcall_binding

Binding object which returns the resources bound to lsnsipalgcall.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
callid	<String>	Read-write	Call ID for the SIP call.
lsnsipalgcall_controlchannel_binding	<lsnsipalgcall_controlchannel_binding[]>	Read-only	controlchannel that can be bound to lsnsipalgcall.
lsnsipalgcall_datachannel_binding	<lsnsipalgcall_datachannel_binding[]>	Read-only	datachannel that can be bound to lsnsipalgcall.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnsipalgcall_binding/ callid_value<String>

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "lsnsipalgcall_binding": [ {

"callid":<String_value>,

"lsnsipalgcall_controlchannel_binding":<lsnsipalgcall_controlchannel_binding[]_value>,

"lsnsipalgcall_datachannel_binding":<lsnsipalgcall_datachannel_binding[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnsipalgcall_binding

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters:

bulkbindings

http:// <netscaler-ip-address> /nitro/v1/config/lsnsipalgcall_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "lsnsipalgcall_binding": [ {

"callid":<String_value>,

"lsnsipalgcall_controlchannel_binding":<lsnsipalgcall_controlchannel_binding[]_value>,

"lsnsipalgcall_datachannel_binding":<lsnsipalgcall_datachannel_binding[]_value>

}]}
```

lsnsipalgcall_controlchannel_binding

Binding object showing the controlchannel that can be bound to lsnsipalgcall.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
callid	<String>	Read-write	Call ID for the SIP call.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
channelip	<String>	Read-write	IP address of the channel.
channelnatport	<Integer>	Read-only	Natted port for the channel.
channelflags	<Integer>	Read-only	Flags for the call entry.
channelprotocol	<String>	Read-only	Channel transport protocol. Possible values = HTTP, FTP, TCP, UDP, SSL, SSL_BRIDGE, SSL_TCP, NNTP, RPCSVR, DNS, ADNS, SNMP, RTSP, DHCPRA, ANY, SIP_UDP, SIP_TCP, SIP_SSL, DNS_TCP, ADNS_TCP, HTTPSVR, HTTPCLIENT, NAT, HA, AAA, SINCTCP, VPN AFTP, MONITORS, SSLVPN UDP, SINCUDP, RIP, UDP CLNT, SASP, RPCCLNTS, ROUTE, AUDIT, STA HTTP, STA SSL, DNS RESOLVE, RDP, MYSQL, MSSQL,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			DIAMETER, SSL_DIAMETER, TFTP, ORACLE, ICA, RADIUS, RADIUSListener, SMPP, PPTP, GRE, SYSLOGTCP, SYSLOGUDP, FIX, SSL_FIX, QUIC, TFTP_DATA, USER_TCP, USER_SSL_TCP, MONGO, MONGO_TLS, MQTT, MQTT_TLS, QUIC_BRIDGE, HTTP_QUIC, CT_TCP, CT_UDP, DOT, ADNS_DOT, ADNS_DOH, KAFKA_BROKER, KAFKA_PRODUCER
channelport	<Integer>	Read-only	port for the channel.
channelnatip	<String>	Read-only	Natted IP address of the channel.
channeltimeout	<Integer>	Read-only	Timeout for the channel.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET

- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnsipalgcall_controlchannel_binding/ callid_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ lsnsipalgcall_controlchannel_binding/ callid_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of lsnsipalgcall_controlchannel_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/lsnsipalgcall_controlchannel_binding/ callid_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the lsnsipalgcall_controlchannel_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lsnsipalgcall_controlchannel_binding": [ {

"callid":<String_value>,

"channelip":<String_value>,

"channelnatport":<Integer_value>,

"channelflags":<Integer_value>,

"channelprotocol":<String_value>,

"channelport":<Integer_value>,

"channelnatip":<String_value>,

"channeltimeout":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnsipalgcall_controlchannel_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/lsnsipalgcall_controlchannel_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lsnsipalgcall_controlchannel_binding": [ {

"callid":<String_value>,

"channelip":<String_value>,

"channelnatport":<Integer_value>,

"channelflags":<Integer_value>,

"channelprotocol":<String_value>,

"channelport":<Integer_value>,

"channelnatip":<String_value>,
```

```
"channeltimeout":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnsipalgcall_controlchannel_binding/ callid_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"lsnsipalgcall_controlchannel_binding": [ { "__count": "#no"} ] }
```

lsnsipalgcall_datachannel_binding

Binding object showing the datachannel that can be bound to lsnsipalgcall.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
callid	<String>	Read-write	Call ID for the SIP call.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
channelip	<String>	Read-write	IP address of the channel.
channeltimeout	<Integer>	Read-only	Timeout for the channel.
channelport	<Integer>	Read-only	port for the channel.
channelnatip	<String>	Read-only	Natted IP address of the channel.
channelflags	<Integer>	Read-only	Flags for the call entry.
channelnatport	<Integer>	Read-only	Natted port for the channel.
channelprotocol	<String>	Read-only	Channel transport protocol. Possible values = HTTP, FTP, TCP, UDP, SSL, SSL_BRIDGE, SSL_TCP, NNTP, RPCSVR, DNS, ADNS, SNMP, RTSP, DHCPRA, ANY, SIP_UDP, SIP_TCP, SIP_SSL, DNS_TCP, ADNS_TCP, HTTPSVR, HTTPCLIENT, NAT, HA, AAA, SINCTCP, VPN AFTP, MONITORS, SSLVPN UDP, SINCUDP, RIP,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			UDP CLNT, SASP, RPCCLNTS, ROUTE, AUDIT, STA HTTP, STA SSL, DNS RESOLVE, RDP, MYSQL, MSSQL, DIAMETER, SSL_DIAMETER, TFTP, ORACLE, ICA, RADIUS, RADIUSListener, SMPP, PPTP, GRE, SYSLOGTCP, SYSLOGUDP, FIX, SSL_FIX, QUIC, TFTP_DATA, USER_TCP, USER_SSL_TCP, MONGO, MONGO_TLS, MQTT, MQTT_TLS, QUIC_BRIDGE, HTTP_QUIC, CT_TCP, CT_UDP, DOT, ADNS_DOT, ADNS_DOH, KAFKA_BROKER, KAFKA_PRODUCER
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnsipalgcall_datachannel_binding/ callid_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ lsnsipalgcall_datachannel_binding/ callid_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of lsnsipalgcall_datachannel_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/lsnsipalgcall_datachannel_binding/callid_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the lsnsipalgcall_datachannel_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lsnsipalgcall_datachannel_binding": [ {

"callid":<String_value>,

"channelip":<String_value>,

"channeltimeout":<Integer_value>,

"channelport":<Integer_value>,

"channelnatip":<String_value>,

"channelflags":<Integer_value>,

"channelnatport":<Integer_value>,

"channelprotocol":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnsipalgcall_datachannel_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/lsnsipalgcall_datachannel_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lsnsipalgcall_datachannel_binding": [ {

"callid":<String_value>,

"channelip":<String_value>,

"channeltimeout":<Integer_value>,

"channelport":<Integer_value>,

"channelnatip":<String_value>,

"channelflags":<Integer_value>,
```

```
"channelnatport":<Integer_value>,

"channelprotocol":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnsipalgcall_datachannel_binding/callid_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"lsnsipalgcall_datachannel_binding": [ { "__count": "#no"} ] }
```

lsnsipalgprofile

Configuration for LSN SIPALG Profile resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
sipalgprofilename	<String>	Read-write	The name of the SIPALG Profile.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum length = 1 Maximum length = 127
datasessionidletimeout	<Integer>	Read-write	Idle timeout for the data channel sessions in seconds. Default value: 120
sipsessiontimeout	<Integer>	Read-write	SIP control channel session timeout in seconds. Default value: 600
registrationtimeout	<Integer>	Read-write	SIP registration timeout in seconds. Default value: 60
sipsrcportrange	<String>	Read-write	Source port range for SIP_UDP and SIP_TCP.
sipdstportrange	<String>	Read-write	Destination port range for SIP_UDP and SIP_TCP.
openregisterpinhole	<String>	Read-write	ENABLE/DISABLE RegisterPinhole creation. Default value: ENABLED Possible values = ENABLED, DISABLED
opencontactpinhole	<String>	Read-write	ENABLE/DISABLE ContactPinhole creation.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: ENABLED Possible values = ENABLED, DISABLED
openviapinhole	<String>	Read-write	ENABLE/DISABLE ViaPinhole creation. Default value: ENABLED Possible values = ENABLED, DISABLED
openrecordroutepinhole	<String>	Read-write	ENABLE/DISABLE RecordRoutePinhole creation. Default value: ENABLED Possible values = ENABLED, DISABLED
siptransportprotocol	<String>	Read-write	SIP ALG Profile transport protocol type. Possible values = TCP, UDP
openroutepinhole	<String>	Read-write	ENABLE/DISABLE RoutePinhole creation. Default value: ENABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ENABLED, DISABLED
rport	<String>	Read-write	ENABLE/DISABLE rport. Default value: ENABLED Possible values = ENABLED, DISABLED
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT
- DELETE

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnsipalgprofile **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"lsnsipalgprofile":{

<b>"sipalgprofilename":<String_value>,

</b>"datasessionidletimeout":<Integer_value>,

"sipsessiontimeout":<Integer_value>,

"registrationtimeout":<Integer_value>,

"sipsrcportrange":<String_value>,

"sipdstportrange":<String_value>,

"openregisterpinhole":<String_value>,
```

```
"opencontactpinhole":<String_value>,

"openviapinhole":<String_value>,

"openrecordroutepinhole":<String_value>,

<b>"siptransportprotocol":<String_value>,

</b>"openroutepinhole":<String_value>,

"rport":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnsipalgprofile **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"lsnsipalgprofile":{

<b>"sipalgprofilename":<String_value>,

</b>"datasessionidletimeout":<Integer_value>,

"sipsessiontimeout":<Integer_value>,

"registrationtimeout":<Integer_value>,

"sipsrcportrange":<String_value>,
```

```
"sipdstportrange":<String_value>,

"openregisterpinhole":<String_value>,

"opencontactpinhole":<String_value>,

"openviapinhole":<String_value>,

"openrecordroutepinhole":<String_value>,

"siptransportprotocol":<String_value>,

"openroutepinhole":<String_value>,

"rport":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnsipalgprofile? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"lsnsipalgprofile":{

<b>"sipalgprofilename":<String_value>,

</b>"datasessionidletimeout":true,
```

```
"sipsessiontimeout":true,

"registrationtimeout":true,

"sipsrcportrange":true,

"sipdstportrange":true,

"openregisterpinhole":true,

"opencontactpinhole":true,

"openviapinhole":true,

"openrecordroutepinhole":true,

"siptransportprotocol":true,

"openroutepinhole":true,

"rport":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnsipalgprofile/ sipalgprofilename_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnsipalgprofile **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/lsnsipalgprofile? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/lsnsipalgprofile? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of lsnsipalgprofile resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/lsnsipalgprofile? **view=summary**

Use this query-parameter to get the summary output of lsnsipalgprofile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/lsnsipalgprofile? **pagesize=#no;pageno=#no**

Use this query-parameter to get the lsnsipalgprofile resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "lsnsipalgprofile": [ {

"sipalgprofilename":<String_value>,

"datasessionidletimeout":<Integer_value>,

"sipsessiontimeout":<Integer_value>,

"registrationtimeout":<Integer_value>,

"sipsrcportrange":<String_value>,

"sipdstportrange":<String_value>,

"openregisterpinhole":<String_value>,

"opencontactpinhole":<String_value>,

"openviapinhole":<String_value>,

"openrecordroutepinhole":<String_value>,

"siptransportprotocol":<String_value>,

"openroutepinhole":<String_value>,

"rport":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnsipalgprofile/ sipalgprofilename_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/ config/lsnsipalgprofile/ sipalgprofilename_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/lsnsipalgprofile/ sipalgprofilename_value<String> ? **view=summary**

Use this query-parameter to get the summary output of lsnsipalgprofile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lsnsipalgprofile": [ {

"sipalgprofilename":<String_value>,

"datasessionidletimeout":<Integer_value>,

"sipsessiontimeout":<Integer_value>,

"registrationtimeout":<Integer_value>,

"sipsrcportrange":<String_value>,

"sipdstportrange":<String_value>,

"openregisterpinhole":<String_value>,

"opencontactpinhole":<String_value>,
```

```
"openviapinhole":<String_value>,

"openrecordroutepinhole":<String_value>,

"siptransportprotocol":<String_value>,

"openroutepinhole":<String_value>,

"rport":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnsipalgprofile? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "lsnsipalgprofile": [ { "__count": "#no"} ] }
```

lsnstatic

Configuration for static mapping resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the LSN static mapping entry. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the LSN group is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "lsn static1" or 'lsn static1'). Minimum length = 1 Maximum length = 127
transportprotocol	<String>	Read-write	Protocol for the LSN mapping entry.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = TCP, UDP, ICMP, ALL
subscrip	<String>	Read-write	IPv4(NAT44 ; DS-Lite)/IPv6(NAT64) address of an LSN subscriber for the LSN static mapping entry.
subscrport	<Integer>	Read-write	Port of the LSN subscriber for the LSN mapping entry. * represents all ports being used. Used in case of static wildcard. Minimum value = 0 Maximum value = 65535 Range 1 - 65535 * in CLI is represented as 65535 in NITRO API
network6	<String>	Read-write	B4 address in DS-Lite setup. Minimum length = 1
td	<Integer>	Read-write	ID of the traffic domain to which the subscriber belongs. If you do not specify an ID, the subscriber is

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			assumed to be a part of the default traffic domain. Default value: 0 Minimum value = 0 Maximum value = 4094
natip	<String>	Read-write	IPv4 address, already existing on the Citrix ADC as type LSN, to be used as NAT IP address for this mapping entry.
natport	<Integer>	Read-write	NAT port for this LSN mapping entry. * represents all ports being used. Used in case of static wildcard. Minimum value = 0 Maximum value = 65535 Range 1 - 65535 * in CLI is represented as 65535 in NITRO API
destip	<String>	Read-write	Destination IP address for the LSN mapping entry.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
dsttd	<Integer>	Read-write	ID of the traffic domain through which the destination IP address for this LSN mapping entry is reachable from the Citrix ADC. If you do not specify an ID, the destination IP address is assumed to be reachable through the default traffic domain, which has an ID of 0. Default value: 0 Minimum value = 0 Maximum value = 4094
nattype	<String>	Read-write	Type of sessions to be displayed. Possible values = NAT44, DS-Lite, NAT64
status	<String>	Read-only	The status of the Mapping. Status could be Inactive, if mapping addition failed due to already existing dynamic/ static mapping, port allocation failure.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ACTIVE, INACTIVE
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnstatic **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"lsnstatic":{

<b>"name":<String_value>,

</b><b>"transportprotocol":<String_value>,

</b><b>"subscrip":<String_value>,

</b><b>"subscrport":<Integer_value>,

</b>"network6":<String_value>,

"td":<Integer_value>,

"natip":<String_value>,

"natport":<Integer_value>,

"destip":<String_value>,

"dsttd":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnstatic/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnstatic **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/lsnstatic? **args=name: <String_value> ,nattype: <String_value>**

Use this query-parameter to get lsnstatic resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/config/lsnstatic? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/lsnstatic? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of lsnstatic resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/lsnstatic? **view=summary**

Use this query-parameter to get the summary output of lsnstatic resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/lsnstatic? **pagesize=#no;pageno=#no**

Use this query-parameter to get the lsnstatic resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "lsnstatic": [ {

name:<String_value>,nattype:<String_value>"transportprotocol":<String_valu
e>,

"subscrip":<String_value>,

"subscrport":<Integer_value>,

"network6":<String_value>,

"natip":<String_value>,

"natport":<Integer_value>,

"td":<Integer_value>,

"destip":<String_value>,

"dsttd":<Integer_value>,

"status":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnstatic/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/lsnstatic/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/lsnstatic/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of lsnstatic resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lsnstatic": [ {

name:<String_value>,nattype:<String_value>"transportprotocol":<String_valu
e>,

"subscrip":<String_value>,

"subscrport":<Integer_value>,

"network6":<String_value>,
```

```
"natip":<String_value>,

"natport":<Integer_value>,

"td":<Integer_value>,

"destip":<String_value>,

"dsttd":<Integer_value>,

"status":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsnstatic? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "lsnstatic": [ { "__count": "#no"} ] }
```

lsntransportprofile

Configuration for LSN Transport Profile resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
transportprofilename	<String>	Read-write	Name for the LSN transport profile. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the LSN transport profile is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "lsn transport profile1" or 'lsn transport profile1'). Minimum length = 1 Maximum length = 127

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
transportprotocol	<String>	Read-write	Protocol for which to set the LSN transport profile parameters. Possible values = TCP, UDP, ICMP
sessiontimeout	<Integer>	Read-write	Timeout, in seconds, for an idle LSN session. If an LSN session is idle for a time that exceeds this value, the Citrix ADC removes the session. This timeout does not apply for a TCP LSN session when a FIN or RST message is received from either of the endpoints. . Default value: 120 Minimum value = 60
finrsttimeout	<Integer>	Read-write	Timeout, in seconds, for a TCP LSN session after a FIN or RST message is received from one of the endpoints. If a TCP LSN session is idle (after the Citrix ADC receives a FIN or RST message) for a time that exceeds this value, the Citrix

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			ADC ADC removes the session. Since the LSN feature of the Citrix ADC does not maintain state information of any TCP LSN sessions, this timeout accommodates the transmission of the FIN or RST, and ACK messages from the other endpoint so that both endpoints can properly close the connection. Default value: 30
stuntimeout	<Integer>	Read-write	STUN protocol timeout. Default value: 600 Minimum value = 120 Maximum value = 1200
synidletimeout	<Integer>	Read-write	SYN Idle timeout. Default value: 60 Minimum value = 30 Maximum value = 120

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
portquota	<Integer>	Read-write	Maximum number of LSN NAT ports to be used at a time by each subscriber for the specified protocol. For example, each subscriber can be limited to a maximum of 500 TCP NAT ports. When the LSN NAT mappings for a subscriber reach the limit, the Citrix ADC does not allocate additional NAT ports for that subscriber. Default value: 0 Minimum value = 0 Maximum value = 65535
sessionquota	<Integer>	Read-write	Maximum number of concurrent LSN sessions allowed for each subscriber for the specified protocol. When the number of LSN sessions reaches the limit for a subscriber, the Citrix ADC does not allow the subscriber to open additional sessions.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: 0 Minimum value = 0 Maximum value = 65535
groupsessionlimit	<Integer>	Read-write	Maximum number of concurrent LSN sessions(for the specified protocol) allowed for all subscriber of a group to which this profile has bound. This limit will get split across the Citrix ADCs packet engines and rounded down. When the number of LSN sessions reaches the limit for a group in packet engine, the Citrix ADC does not allow the subscriber of that group to open additional sessions through that packet engine. Default value: 0
portpreserveparity	<String>	Read-write	Enable port parity between a subscriber port and its mapped LSN NAT port. For example, if a subscriber initiates a connection from an odd numbered port, the Citrix ADC

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			allocates an odd numbered LSN NAT port for this connection. You must set this parameter for proper functioning of protocols that require the source port to be even or odd numbered, for example, in peer-to-peer applications that use RTP or RTCP protocol. Default value: DISABLED Possible values = ENABLED, DISABLED
portpreserverange	<String>	Read-write	If a subscriber initiates a connection from a well-known port (0-1023), allocate a NAT port from the well-known port range (0-1023) for this connection. For example, if a subscriber initiates a connection from port 80, the Citrix ADC can allocate port 100 as the NAT port for this connection.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			This parameter applies to dynamic NAT without port block allocation. It also applies to Deterministic NAT if the range of ports allocated includes well-known ports. When all the well-known ports of all the available NAT IP addresses are used in different subscriber's connections (LSN sessions), and a subscriber initiates a connection from a well-known port, the Citrix ADC drops this connection. Default value: DISABLED Possible values = ENABLED, DISABLED
syncheck	<String>	Read-write	Silently drop any non-SYN packets for connections for which there is no LSN-NAT session present on the Citrix ADC.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			If you disable this parameter, the Citrix ADC accepts any non-SYN packets and creates a new LSN session entry for this connection. Following are some reasons for the Citrix ADC to receive such packets: * LSN session for a connection existed but the Citrix ADC removed this session because the LSN session was idle for a time that exceeded the configured session timeout. * Such packets can be a part of a DoS attack. Default value: ENABLED Possible values = ENABLED, DISABLED
_nextgenapiresource	<String>	Read-only	.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsntransportprofile **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"lsntransportprofile":{

<b>"transportprofilename":<String_value>,

</b><b>"transportprotocol":<String_value>,

</b>"sessiontimeout":<Integer_value>,

"finrsttimeout":<Integer_value>,

"stuntimeout":<Integer_value>,

"synidletimeout":<Integer_value>,

"portquota":<Integer_value>,

"sessionquota":<Integer_value>,

"groupsessionlimit":<Integer_value>,

"portpreserveparity":<String_value>,

"portpreserverange":<String_value>,

"syncheck":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsntransportprofile/transportprofilename_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsntransportprofile **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"lsntransportprofile":{

<b>"transportprofilename":<String_value>,

</b>"sessiontimeout":<Integer_value>,

"finrsttimeout":<Integer_value>,

"stuntimeout":<Integer_value>,

"synidletimeout":<Integer_value>,

"portquota":<Integer_value>,

"sessionquota":<Integer_value>,

"groupsessionlimit":<Integer_value>,
```

```
"portpreserveparity":<String_value>,

"portpreserverange":<String_value>,

"syncheck":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsntransportprofile? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"lsntransportprofile":{

<b>"transportprofilename":<String_value>,

</b>"sessiontimeout":true,

"finrsttimeout":true,

"stuntimeout":true,

"synidletimeout":true,

"portquota":true,

"sessionquota":true,
```

```
"groupsessionlimit":true,

"portpreserveparity":true,

"portpreserverange":true,

"syncheck":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsntransportprofile **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/lsntransportprofile? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/lsntransportprofile? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of lsntransportprofile resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/lsntransportprofile? **view=summary**

Use this query-parameter to get the summary output of lsntransportprofile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/lsntransportprofile? **pagesize=#no;pageno=#no**

Use this query-parameter to get the lsntransportprofile resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "lsntransportprofile": [ {

"transportprofilename":<String_value>,

"transportprotocol":<String_value>,

"sessiontimeout":<Integer_value>,

"finrsttimeout":<Integer_value>,

"stuntimeout":<Integer_value>,

"synidletimeout":<Integer_value>,

"portquota":<Integer_value>,

"sessionquota":<Integer_value>,

"groupsessionlimit":<Integer_value>,

"portpreserveparity":<String_value>,

"portpreserverange":<String_value>,

"syncheck":<String_value>,

"_nextgenapiresource":<String_value>
```

```
}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsntransportprofile/ transportprofilename_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/lsntransportprofile/ transportprofilename_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/lsntransportprofile/ transportprofilename_value<String> ? **view=summary**

Use this query-parameter to get the summary output of lsntransportprofile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lsntransportprofile": [ {

"transportprofilename":<String_value>,

"transportprotocol":<String_value>,
```

```
"sessiontimeout":<Integer_value>,

"finrsttimeout":<Integer_value>,

"stuntimeout":<Integer_value>,

"synidletimeout":<Integer_value>,

"portquota":<Integer_value>,

"sessionquota":<Integer_value>,

"groupsessionlimit":<Integer_value>,

"portpreserveparity":<String_value>,

"portpreserverange":<String_value>,

"syncheck":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/lsntransportprofile? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "lsntransportprofile": [ { "__count": "#no"} ] }
```

metrics

Metrics

Metrics configuration.

NAME	DESCRIPTION
metricsprofile	Configuration for Metrics profile
metricsprofile_authenticationvserver_binding	Binding object showing the authenticationvserver that can be bound to metricsprofile
metricsprofile_binding	Binding object showing the resources that can be bound to metricsprofile
metricsprofile_crvserver_binding	Binding object showing the crvserver that can be bound to metricsprofile
metricsprofile_csvserver_binding	Binding object showing the csvserver that can be bound to metricsprofile
metricsprofile_gslbvserver_binding	Binding object showing the gslbvserver that can be bound to metricsprofile
metricsprofile_lbvserver_binding	Binding object showing the lbvserver that can be bound to metricsprofile

NAME	DESCRIPTION
metricsprofile_service_binding	Binding object showing the service that can be bound to metricsprofile
metricsprofile_servicegroup_binding	Binding object showing the servicegroup that can be bound to metricsprofile
metricsprofile_uservserver_binding	Binding object showing the uservserver that can be bound to metricsprofile
metricsprofile_vpnvserver_binding	Binding object showing the vpnvserver that can be bound to metricsprofile

metricsprofile

Configuration for Metrics profile resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the metrics profile. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters.!.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum length = 1 Maximum length = 127
collector	<String>	Read-write	The collector should be a HTTP/HTTPS service. . Minimum length = 1
outputmode	<String>	Read-write	This option indicates the format in which metrics data is generated. Default value: avro, Possible values = avro, prometheus, influx, json
metrics	<String>	Read-write	This option is used enable or disable metrics . Default value: DISABLED Possible values = ENABLED, DISABLED
servemode	<String>	Read-write	This option is to configure metrics pull or push mode. In push mode metricscollector exports metrics to configured collector. In pull mode, metricscollector only generates the metrics which will be

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			pulled by external agent. No collector configuration is required in pull mode and it is applicable only for output mode Prometheus. Default value: Push Possible values = Push, Pull
schemafile	<String>	Read-write	This option is for configuring json schema file containing a list of counters to be exported by metricscollector. Schema file should be present under /var/metrics_conf path. Maximum length = 64
metricsexportfrequency	<Integer>	Read-write	This option is for configuring the metrics export frequency in seconds, frequency value must be in [30,300] seconds range. Default value: 30 Minimum value = 30 Maximum value = 300

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
metricsauthtoken	<String>	Read-write	Token for authenticating with the endpoint. If the endpoint requires the Authorization header in a particular format, specify the complete format as the value to this parameter. For eg., in case of splunk, the Authorizaiton header is required to be of the form - Splunk <auth-token>. Maximum length = 512
metricsendpointurl	<String>	Read-write	The URL at which to upload the metrics data on the endpoint. Maximum length = 256
refcnt	<Integer>	Read-only	The number of references to the profile.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- UPDATE
- UNSET
- DELETE

- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/metricsprofile **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"metricsprofile":{

<b>"name":<String_value>,

</b>"collector":<String_value>,

"outputmode":<String_value>,

"metrics":<String_value>,

"servemode":<String_value>,

"schemafile":<String_value>,

"metricsexportfrequency":<Integer_value>,

"metricsauthtoken":<String_value>,

"metricsendpointurl":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/metricsprofile **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"metricsprofile":{

<b>"name":<String_value>,
```

```
</b>"collector":<String_value>,

"outputmode":<String_value>,

"metrics":<String_value>,

"servemode":<String_value>,

"schemafile":<String_value>,

"metricsexportfrequency":<Integer_value>,

"metricsauthtoken":<String_value>,

"metricsendpointurl":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/metricsprofile? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"metricsprofile":{

<b>"name":<String_value>,

</b>"collector":true,
```

```
"outputmode":true,

"metrics":true,

"servemode":true,

"schemafile":true,

"metricsexportfrequency":true,

"metricsauthtoken":true,

"metricsendpointurl":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/metricsprofile/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/metricsprofile **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/metricsprofile? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/metricsprofile? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of metricsprofile resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/metricsprofile? **view=summary**

Use this query-parameter to get the summary output of metricsprofile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/metricsprofile? **pagesize=#no;pageno=#no**

Use this query-parameter to get the metricsprofile resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "metricsprofile": [ {

"name":<String_value>,

"collector":<String_value>,

"refcnt":<Integer_value>,

"outputmode":<String_value>,

"metrics":<String_value>,
```

```
"servemode":<String_value>,

"schemafile":<String_value>,

"metricsexportfrequency":<Integer_value>,

"metricsauthtoken":<String_value>,

"metricsendpointurl":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/metricsprofile/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/metricsprofile/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/metricsprofile/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of metricsprofile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "metricsprofile": [ {

"name":<String_value>,

"collector":<String_value>,

"refcnt":<Integer_value>,

"outputmode":<String_value>,

"metrics":<String_value>,

"servemode":<String_value>,

"schemafile":<String_value>,

"metricsexportfrequency":<Integer_value>,

"metricsauthtoken":<String_value>,

"metricsendpointurl":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/metricsprofile? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "metricsprofile": [ { "__count": "#no"} ] }
```

metricsprofile_authenticationvserver_binding

Binding object showing the authenticationvserver that can be bound to metricsprofile.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
entitytype	<String>	Read-write	Type of the entity bound to the metrics profile. Possible values = lbvserver, csvserver, crvserver, vpnvserver, authvserver, gslbvserver, uservserver, service, servicegroup
name	<String>	Read-write	Name for the metrics profile. Must begin with an ASCII alphabetic or underscore (_)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters.!. Minimum length = 1 Maximum length = 127
entityname	<String>	Read-write	Name of the entity bound to the metrics profile. Minimum length = 1 Maximum length = 127
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT
- ADD
- DELETE

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/metricsprofile_authenticationvserver_binding
HTTP Method: PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"metricsprofile_authenticationvserver_binding":{

<b>"name":<String_value>,

</b>"entityname":<String_value>,

"entitytype":<String_value>
```

```
}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/metricsprofile_authenticationvserver_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ metricsprofile_authenticationvserver_binding/ name_value<String> ? **args=entityname: <String_value> ,entitytype: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/metricsprofile_authenticationvserver_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ metricsprofile_authenticationvserver_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of metricsprofile_authenticationvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ metricsprofile_authenticationvserver_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the metricsprofile_authenticationvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "metricsprofile_authenticationvserver_binding": [ {

"entitytype":<String_value>,

"name":<String_value>,

"entityname":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/metricsprofile_authenticationvserver_binding
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/metricsprofile_authenticationvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "metricsprofile_authenticationvserver_binding": [ {

"entitytype":<String_value>,

"name":<String_value>,

"entityname":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/metricsprofile_authenticationvserver_binding/name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"metricsprofile_authenticationvserver_binding": [ { "__count": "#no"} ] }
```

metricsprofile_binding

Binding object which returns the resources bound to metricsprofile.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the profile about which to display information. Minimum length = 1 Maximum length = 127
metricsprofile_csvserver_binding	<metricsprofile_csvserver_binding[]>	Read-only	csvserver that can be bound to metricsprofile.
metricsprofile_vpnvserver_binding	<metricsprofile_vpnvserver_binding[]>	Read-only	vpnvserver that can be bound to metricsprofile.
metricsprofile_gslbvserver_binding	<metricsprofile_gslbvserver_binding[]>	Read-only	gslbvserver that can be bound to metricsprofile.
metricsprofile_servicegroup_binding	<metricsprofile_servicegroup_binding[]>	Read-only	servicegroup that can be bound to metricsprofile.
metricsprofile_authenticationvserver_binding	<metricsprofile_authenticationvserver_binding[]>	Read-only	authenticationvserver that can be bound to metricsprofile.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
metricsprofile_crvserver_binding	<metricsprofile_crvserver_binding[]>	Read-only	crvserver that can be bound to metricsprofile.
metricsprofile_uservserver_binding	<metricsprofile_uservserver_binding[]>	Read-only	uservserver that can be bound to metricsprofile.
metricsprofile_lbvserver_binding	<metricsprofile_lbvserver_binding[]>	Read-only	lbvserver that can be bound to metricsprofile.
metricsprofile_service_binding	<metricsprofile_service_binding[]>	Read-only	service that can be bound to metricsprofile.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/metricsprofile_binding/ name_value<String>
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "metricsprofile_binding": [ {

"name":<String_value>,

"metricsprofile_servicegroup_binding":<metricsprofile_servicegroup_binding
[]_value>,

"metricsprofile_gslbvserver_binding":<metricsprofile_gslbvserver_binding[]
_value>,

"metricsprofile_service_binding":<metricsprofile_service_binding[]_value>,

"metricsprofile_authenticationvserver_binding":<metricsprofile_authenticat
ionvserver_binding[]_value>,
```

```
"metricsprofile_csvserver_binding":<metricsprofile_csvserver_binding[]_value>,

"metricsprofile_crvserver_binding":<metricsprofile_crvserver_binding[]_value>,

"metricsprofile_vpnvserver_binding":<metricsprofile_vpnvserver_binding[]_value>,

"metricsprofile_uservserver_binding":<metricsprofile_uservserver_binding[]_value>,

"metricsprofile_lbvserver_binding":<metricsprofile_lbvserver_binding[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/metricsprofile_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/metricsprofile_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "metricsprofile_binding": [ {

"name":<String_value>,

"metricsprofile_servicegroup_binding":<metricsprofile_servicegroup_binding
[]_value>,

"metricsprofile_gslbvserver_binding":<metricsprofile_gslbvserver_binding[]
_value>,

"metricsprofile_service_binding":<metricsprofile_service_binding[]_value>,

"metricsprofile_authenticationvserver_binding":<metricsprofile_authenticat
ionvserver_binding[]_value>,

"metricsprofile_csvserver_binding":<metricsprofile_csvserver_binding[]_val
ue>,

"metricsprofile_crvserver_binding":<metricsprofile_crvserver_binding[]_val
ue>,

"metricsprofile_vpnvserver_binding":<metricsprofile_vpnvserver_binding[]_v
alue>,

"metricsprofile_uservserver_binding":<metricsprofile_uservserver_binding[]
_value>,

"metricsprofile_lbvserver_binding":<metricsprofile_lbvserver_binding[]_val
ue>

}]}
```

metricsprofile_crvserver_binding

Binding object showing the crvserver that can be bound to metricsprofile.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the metrics profile. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters.!. Minimum length = 1 Maximum length = 127
entityname	<String>	Read-write	Name of the entity bound to the metrics profile. Minimum length = 1 Maximum length = 127
entitytype	<String>	Read-write	Type of the entity bound to the metrics profile. Possible values = lbvserver, csvserver, crvserver, vpnvserver, authvserver, gslbvserver, uservserver,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			service, servicegroup
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT
- ADD
- DELETE

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/metricsprofile_crvserver_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"metricsprofile_crvserver_binding":{

<b>"name":<String_value>,

</b>"entityname":<String_value>,

"entitytype":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/metricsprofile_crvserver_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ metricsprofile_crvserver_binding/ name_value<String> ? **args=entityname: <String_value> ,entitytype: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/metricsprofile_crvserver_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ metricsprofile_crvserver_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of metricsprofile_crvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/metricsprofile_crvserver_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the metricsprofile_crvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "metricsprofile_crvserver_binding": [ {

"name":<String_value>,

"entityname":<String_value>,
```

```
"entitytype":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/metricsprofile_crvserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/metricsprofile_crvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "metricsprofile_crvserver_binding": [ {

"name":<String_value>,

"entityname":<String_value>,

"entitytype":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/metricsprofile_crvserver_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"metricsprofile_crvserver_binding": [ { "__count": "#no"} ] }
```

metricsprofile_csvserver_binding

Binding object showing the csvserver that can be bound to metricsprofile.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
entitytype	<String>	Read-write	Type of the entity bound to the metrics profile. Possible values = lbvserver, csvserver, crvserver,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			vpnvserver, authvserver, gslbvserver, uservserver, service, servicegroup
name	<String>	Read-write	Name for the metrics profile. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters.!. Minimum length = 1 Maximum length = 127
entityname	<String>	Read-write	Name of the entity bound to the metrics profile. Minimum length = 1 Maximum length = 127
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- GET

- GET (ALL)
- COUNT
- ADD
- DELETE

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/metricsprofile_csvserver_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"metricsprofile_csvserver_binding":{

<b>"name":<String_value>,

</b>"entityname":<String_value>,

"entitytype":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/metricsprofile_csvserver_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ metricsprofile_csvserver_binding/ name_value<String> ? **args=entityname: <String_value> ,entitytype: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/metricsprofile_csvserver_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ metricsprofile_csvserver_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of metricsprofile_csvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/metricsprofile_csvserver_binding/name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the metricsprofile_csvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "metricsprofile_csvserver_binding": [ {

"entitytype":<String_value>,

"name":<String_value>,

"entityname":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/metricsprofile_csvserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/metricsprofile_csvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "metricsprofile_csvserver_binding": [ {

"entitytype":<String_value>,

"name":<String_value>,

"entityname":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/metricsprofile_csvserver_binding/name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"metricsprofile_csvserver_binding": [ { "__count": "#no"} ] }
```

metricsprofile_gslbvserver_binding

Binding object showing the gslbvserver that can be bound to metricsprofile.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
entityname	<String>	Read-write	Name of the entity bound to the metrics profile. Minimum length = 1 Maximum length = 127
name	<String>	Read-write	Name for the metrics profile. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			hyphen (-) characters.!. Minimum length = 1 Maximum length = 127
entitytype	<String>	Read-write	Type of the entity bound to the metrics profile. Possible values = lbvserver, csvserver, crvserver, vpnvserver, authvserver, gslbvserver, uservserver, service, servicegroup
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT
- ADD
- DELETE

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/metricsprofile_gslbvserver_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"metricsprofile_gslbvserver_binding":{

<b>"name":<String_value>,

</b>"entityname":<String_value>,

"entitytype":<String_value>
```

```
}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/metricsprofile_gslbvserver_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ metricsprofile_gslbvserver_binding/ name_value<String> ? **args=entityname: <String_value> ,entitytype: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/metricsprofile_gslbvserver_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ metricsprofile_gslbvserver_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of metricsprofile_gslbvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/metricsprofile_gslbvserver_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the metricsprofile_gslbvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "metricsprofile_gslbvserver_binding": [ {

"entityname":<String_value>,

"name":<String_value>,

"entitytype":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/metricsprofile_gslbvserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/metricsprofile_gslbvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "metricsprofile_gslbvserver_binding": [ {

"entityname":<String_value>,

"name":<String_value>,

"entitytype":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/metricsprofile_gslbvserver_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"metricsprofile_gslbvserver_binding": [ { "__count": "#no"} ] }
```

metricsprofile_lbvserver_binding

Binding object showing the lbvserver that can be bound to metricsprofile.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
entitytype	<String>	Read-write	Type of the entity bound to the metrics profile. Possible values = lbvserver, csvserver, crvserver, vpnvserver, authvserver, gslbvserver, uservserver, service, servicegroup
entityname	<String>	Read-write	Name of the entity bound to the metrics profile. Minimum length = 1 Maximum length = 127
name	<String>	Read-write	Name for the metrics profile. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@),

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			equals (=), and hyphen (-) characters.!. Minimum length = 1 Maximum length = 127
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT
- ADD
- DELETE

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/metricsprofile_lbvserver_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"metricsprofile_lbvserver_binding":{

<b>"name":<String_value>,

</b>"entityname":<String_value>,

"entitytype":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/metricsprofile_lbvserver_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ metricsprofile_lbvserver_binding/ name_value<String> ? **args=entityname: <String_value> ,entitytype: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/metricsprofile_lbvserver_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ metricsprofile_lbvserver_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of metricsprofile_lbvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/metricsprofile_lbvserver_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the metricsprofile_lbvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "metricsprofile_lbvserver_binding": [ {

"entitytype":<String_value>,

"entityname":<String_value>,

"name":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/metricsprofile_lbvserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/metricsprofile_lbvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "metricsprofile_lbvserver_binding": [ {

"entitytype":<String_value>,
```

```
"entityname":<String_value>,

"name":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/metricsprofile_lbvserver_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"metricsprofile_lbvserver_binding": [ { "__count": "#no"} ] }
```

metricsprofile_service_binding

Binding object showing the service that can be bound to metricsprofile.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
entityname	<String>	Read-write	Name of the entity bound to the metrics profile. Minimum length = 1 Maximum length = 127
name	<String>	Read-write	Name for the metrics profile. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters.!. Minimum length = 1 Maximum length = 127
entitytype	<String>	Read-write	Type of the entity bound to the metrics profile. Possible values = lbvserver, csvserver, crvserver, vpnvserver, authvserver, gslbvserver, uservserver,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			service, servicegroup
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT
- ADD
- DELETE

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/metricsprofile_service_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"metricsprofile_service_binding":{

<b>"name":<String_value>,

</b>"entityname":<String_value>,

"entitytype":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/metricsprofile_service_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ metricsprofile_service_binding/ name_value<String> ? **args=entityname: <String_value> ,entitytype: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/metricsprofile_service_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ metricsprofile_service_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of metricsprofile_service_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/metricsprofile_service_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the metricsprofile_service_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "metricsprofile_service_binding": [ {

"entityname":<String_value>,

"name":<String_value>,
```

```
"entitytype":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/metricsprofile_service_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/metricsprofile_service_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "metricsprofile_service_binding": [ {

"entityname":<String_value>,

"name":<String_value>,

"entitytype":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/metricsprofile_service_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"metricsprofile_service_binding": [ { "__count": "#no"} ] }
```

metricsprofile_servicegroup_binding

Binding object showing the servicegroup that can be bound to metricsprofile.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
entitytype	<String>	Read-write	Type of the entity bound to the metrics profile. Possible values = lbvserver, csvserver, crvserver,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			vpnvserver, authvserver, gslbvserver, uservserver, service, servicegroup
entityname	<String>	Read-write	Name of the entity bound to the metrics profile. Minimum length = 1 Maximum length = 127
name	<String>	Read-write	Name for the metrics profile. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters.!. Minimum length = 1 Maximum length = 127
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- GET

- GET (ALL)
- COUNT
- ADD
- DELETE

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/metricsprofile_servicegroup_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"metricsprofile_servicegroup_binding":{

<b>"name":<String_value>,

</b>"entityname":<String_value>,

"entitytype":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/metricsprofile_servicegroup_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ metricsprofile_servicegroup_binding/ name_value<String> ? **args=entityname: <String_value> ,entitytype: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/metricsprofile_servicegroup_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ metricsprofile_servicegroup_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of metricsprofile_servicegroup_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/metricsprofile_servicegroup_binding/name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the metricsprofile_servicegroup_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "metricsprofile_servicegroup_binding": [ {

"entitytype":<String_value>,

"entityname":<String_value>,

"name":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/metricsprofile_servicegroup_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/metricsprofile_servicegroup_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "metricsprofile_servicegroup_binding": [ {

"entitytype":<String_value>,

"entityname":<String_value>,

"name":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/metricsprofile_servicegroup_binding/name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"metricsprofile_servicegroup_binding": [ { "__count": "#no"} ] }
```

metricsprofile_uservserver_binding

Binding object showing the uservserver that can be bound to metricsprofile.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
entitytype	<String>	Read-write	Type of the entity bound to the metrics profile. Possible values = lbvserver, csvserver, crvserver, vpnvserver, authvserver, gslbvserver, uservserver, service, servicegroup
name	<String>	Read-write	Name for the metrics profile. Must begin with an ASCII alphabetic or underscore (_) character, and must

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters.!. Minimum length = 1 Maximum length = 127
entityname	<String>	Read-write	Name of the entity bound to the metrics profile. Minimum length = 1 Maximum length = 127
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT
- ADD
- DELETE

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/metricsprofile_uservserver_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"metricsprofile_uservserver_binding":{

<b>"name":<String_value>,

</b>"entityname":<String_value>,

"entitytype":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/metricsprofile_uservserver_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ metricsprofile_uservserver_binding/ name_value<String> ? **args=entityname: <String_value> ,entitytype: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/metricsprofile_uservserver_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ metricsprofile_uservserver_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of metricsprofile_uservserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/metricsprofile_uservserver_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the metricsprofile_uservserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "metricsprofile_uservserver_binding": [ {

"entitytype":<String_value>,

"name":<String_value>,

"entityname":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/metricsprofile_uservserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/metricsprofile_uservserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "metricsprofile_uservserver_binding": [ {

"entitytype":<String_value>,

"name":<String_value>,

"entityname":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/metricsprofile_uservserver_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"metricsprofile_uservserver_binding": [ { "__count": "#no"} ] }
```

metricsprofile_vpnvserver_binding

Binding object showing the vpnvserver that can be bound to metricsprofile.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
entitytype	<String>	Read-write	Type of the entity bound to the metrics profile. Possible values = lbvserver, csvserver, crvserver, vpnvserver, authvserver, gslbvserver, uservserver, service, servicegroup
name	<String>	Read-write	Name for the metrics profile. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters.!. Minimum length = 1 Maximum length = 127

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
entityname	<String>	Read-write	Name of the entity bound to the metrics profile. Minimum length = 1 Maximum length = 127
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT
- ADD
- DELETE

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/metricsprofile_vpnvserver_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"metricsprofile_vpnvserver_binding":{

<b>"name":<String_value>,

</b>"entityname":<String_value>,

"entitytype":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/metricsprofile_vpnvserver_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ metricsprofile_vpnvserver_binding/ name_value<String> ? **args=entityname: <String_value> ,entitytype: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/metricsprofile_vpnvserver_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ metricsprofile_vpnvserver_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of metricsprofile_vpnvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/metricsprofile_vpnvserver_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the metricsprofile_vpnvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "metricsprofile_vpnvserver_binding": [ {

"entitytype":<String_value>,

"name":<String_value>,

"entityname":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/metricsprofile_vpnvserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/metricsprofile_vpnvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "metricsprofile_vpnvserver_binding": [ {

"entitytype":<String_value>,
```

```
"name":<String_value>,

"entityname":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/metricsprofile_vpnvserver_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"metricsprofile_vpnvserver_binding": [ { "__count": "#no"} ] }
```

network

Network

Networking commands.

NAME	DESCRIPTION
Interface	Configuration for interface

NAME	DESCRIPTION
appalgparam	Configuration for AppAlg Param
arp	Configuration for arp
arpparam	Configuration for Global arp parameters
bridgegroup	Configuration for bridge group
bridgegroup_binding	Binding object showing the resources that can be bound to bridgegroup
bridgegroup_nsip6_binding	Binding object showing the nsip6 that can be bound to bridgegroup
bridgegroup_nsip_binding	Binding object showing the nsip that can be bound to bridgegroup
bridgegroup_vlan_binding	Binding object showing the vlan that can be bound to bridgegroup
bridgetable	Configuration for bridge table entry
channel	Configuration for channel
channel_binding	Binding object showing the resources that can be bound to channel
channel_interface_binding	Binding object showing the interface that can be bound to channel

NAME	DESCRIPTION
ci	Configuration for "CI"
fis	Configuration for "FIS"
fis_binding	Binding object showing the resources that can be bound to fis
fis_channel_binding	Binding object showing the channel that can be bound to fis
fis_interface_binding	Binding object showing the interface that can be bound to fis
forwardingsession	Configuration for session forward
inat	Configuration for inbound nat
inatparam	Configuration for INAT parameter
interfacepair	Configuration for "Interface Pair"
ip6tunnel	Configuration for ip6 Tunnel
ip6tunnelparam	Configuration for ip6 tunnel parameter
ipset	Configuration for network ipset
ipset_binding	Binding object showing the resources that can be bound to ipset

NAME	DESCRIPTION
ipset_nsip6_binding	Binding object showing the nsip6 that can be bound to ipset
ipset_nsip_binding	Binding object showing the nsip that can be bound to ipset
iptunnel	Configuration for ip Tunnel
iptunnelparam	Configuration for ip tunnel parameter
ipv6	Configuration for ip v6
l2param	Configuration for Layer 2 related parameter
l3param	Configuration for Layer 3 related parameter
l4param	Configuration for Layer 4 related parameter
lacp	Configuration for Link aggregation control protocol
linkset	Configuration for link set
linkset_binding	Binding object showing the resources that can be bound to linkset
linkset_channel_binding	Binding object showing the channel that can be bound to linkset

NAME	DESCRIPTION
linkset_interface_binding	Binding object showing the interface that can be bound to linkset
mapbmr	Configuration for MAP-T Basic Mapping rule
mapbmr_binding	Binding object showing the resources that can be bound to mapbmr
mapbmr_bmrv4network_binding	Binding object showing the bmrv4network that can be bound to mapbmr
mapdmr	Configuration for MAP-T Default Mapping rule
mapdomain	Configuration for MAP-T Map Domain
mapdomain_binding	Binding object showing the resources that can be bound to mapdomain
mapdomain_mapbmr_binding	Binding object showing the mapbmr that can be bound to mapdomain
nat64	Configuration for nat64 config
nat64param	Configuration for NAT64 parameter
nd6	Configuration for nd6
nd6ravariables	Configuration for nd6 Router Advertisment configuration variables

NAME	DESCRIPTION
nd6ravariables_binding	Binding object showing the resources that can be bound to nd6ravariables
nd6ravariables_onlinkipv6prefix_binding	Binding object showing the onlinkipv6prefix that can be bound to nd6ravariables
netbridge	Configuration for network bridge
netbridge_binding	Binding object showing the resources that can be bound to netbridge
netbridge_iptunnel_binding	Binding object showing the iptunnel that can be bound to netbridge
netbridge_nsip6_binding	Binding object showing the nsip6 that can be bound to netbridge
netbridge_nsip_binding	Binding object showing the nsip that can be bound to netbridge
netbridge_vlan_binding	Binding object showing the vlan that can be bound to netbridge
netprofile	Configuration for Network profile
netprofile_binding	Binding object showing the resources that can be bound to netprofile
netprofile_natrule_binding	Binding object showing the natrule that can be bound to netprofile

NAME	DESCRIPTION
netprofile_srcportset_binding	Binding object showing the srcportset that can be bound to netprofile
onlinkipv6prefix	Configuration for on-link IPv6 global prefixes for Router Advertisment
portallocation	Configuration for portallocation
ptp	Configuration for Precision Time Protocol
rnat	Configuration for RNAT configured route
rnat6	Configuration for IPv6 RNAT configured route
rnat6_binding	Binding object showing the resources that can be bound to rnat6
rnat6_nsip6_binding	Binding object showing the nsip6 that can be bound to rnat6
rnat_binding	Binding object showing the resources that can be bound to rnat
rnat_nsip_binding	Binding object showing the nsip that can be bound to rnat
rnat_retainsourceportset_binding	Binding object showing the retainsourceportset that can be bound to rnat

NAME	DESCRIPTION
rnatglobal_auditsyslogpolicy_binding	Binding object showing the auditsyslogpolicy that can be bound to rnatglobal
rnatglobal_binding	Binding object showing the resources that can be bound to rnatglobal
rnatparam	Configuration for RNAT parameter
rnatsession	Configuration for RNAT session
route	Configuration for route
route6	Configuration for route 6
rsskeytype	Configuration for RSS key type
vlan	Configuration for "VLAN"
vlan_binding	Binding object showing the resources that can be bound to vlan
vlan_channel_binding	Binding object showing the channel that can be bound to vlan
vlan_interface_binding	Binding object showing the interface that can be bound to vlan
vlan_linkset_binding	Binding object showing the linkset that can be bound to vlan

NAME	DESCRIPTION
vlan_nsip6_binding	Binding object showing the nsip6 that can be bound to vlan
vlan_nsip_binding	Binding object showing the nsip that can be bound to vlan
vrid	Configuration for Virtual Router ID
vrid6	Configuration for Virtual Router ID for IPv6
vrid6_binding	Binding object showing the resources that can be bound to vrid6
vrid6_channel_binding	Binding object showing the channel that can be bound to vrid6
vrid6_interface_binding	Binding object showing the interface that can be bound to vrid6
vrid6_nsip6_binding	Binding object showing the nsip6 that can be bound to vrid6
vrid6_nsip_binding	Binding object showing the nsip that can be bound to vrid6
vrid6_trackinterface_binding	Binding object showing the trackinterface that can be bound to vrid6
vrid_binding	Binding object showing the resources that can be bound to vrid

NAME	DESCRIPTION
vrid_channel_binding	Binding object showing the channel that can be bound to vrid
vrid_interface_binding	Binding object showing the interface that can be bound to vrid
vrid_nsip6_binding	Binding object showing the nsip6 that can be bound to vrid
vrid_nsip_binding	Binding object showing the nsip that can be bound to vrid
vrid_trackinterface_binding	Binding object showing the trackinterface that can be bound to vrid
vridparam	Configuration for VR ID parameter
vxlan	Configuration for "VXLAN"
vxlan_binding	Binding object showing the resources that can be bound to vxlan
vxlan_iptunnel_binding	Binding object showing the iptunnel that can be bound to vxlan
vxlan_nsip6_binding	Binding object showing the nsip6 that can be bound to vxlan
vxlan_nsip_binding	Binding object showing the nsip that can be bound to vxlan

NAME	DESCRIPTION
vxlan_srcip_binding	Binding object showing the srcip that can be bound to vxlan
vxlanvlanmap	Configuration for vxlan vlan mapping
vxlanvlanmap_binding	Binding object showing the resources that can be bound to vxlanvlanmap
vxlanvlanmap_vxlan_binding	Binding object showing the vxlan that can be bound to vxlanvlanmap

Interface

Configuration for interface resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
id	<String>	Read-write	Interface number, in C/U format, where C can take one of the following values: * 0 - Indicates a management interface. * 1 - Indicates a 1 Gbps port. * 10 - Indicates a 10 Gbps port.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			* LA - Indicates a link aggregation port. * LO - Indicates a loop back port. U is a unique integer for representing an interface in a particular port group.
speed	<String>	Read-write	Ethernet speed of the interface, in Mbps. Notes: * If you set the speed as AUTO, the Citrix ADC attempts to auto-negotiate or auto-sense the link speed of the interface when it is UP. You must enable auto negotiation on the interface. * If you set a speed other than AUTO, you must specify the same speed for the peer network device. Mismatched speed and duplex

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			settings between the peer devices of a link lead to link errors, packet loss, and other errors. Some interfaces do not support certain speeds. If you specify an unsupported speed, an error message appears. Default value: AUTO Possible values = AUTO, 10, 100, 1000, 10000, 25000, 40000, 50000, 100000, 200000
duplex	<String>	Read-write	The duplex mode for the interface. Notes:* If you set the duplex mode to AUTO, the Citrix ADC attempts to auto-negotiate the duplex mode of the interface when it is UP. You must enable auto negotiation on the interface. If you set a duplex mode other than AUTO, you must specify the same duplex mode

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			for the peer network device. Mismatched speed and duplex settings between the peer devices of a link lead to link errors, packet loss, and other errors. Default value: AUTO Possible values = AUTO, HALF, FULL
flowctl	<String>	Read-write	802.3x flow control setting for the interface. The 802.3x specification does not define flow control for 10 Mbps and 100 Mbps speeds, but if a Gigabit Ethernet interface operates at those speeds, the flow control settings can be applied. The flow control setting that is finally applied to an interface depends on auto-negotiation. With the ON option, the peer negotiates the flow control, but the appliance then forces two-way flow control for the interface. Default value: OFF

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = OFF, RX, TX, RXTX, ON
autoneg	<String>	Read-write	Auto-negotiation state of the interface. With the ENABLED setting, the Citrix ADC auto-negotiates the speed and duplex settings with the peer network device on the link. The Citrix ADC appliance auto-negotiates the settings of only those parameters (speed or duplex mode) for which the value is set as AUTO. Default value: NSA_DVC_AUTONEG_ON Possible values = DISABLED, ENABLED
hamonitor	<String>	Read-write	In a High Availability (HA) configuration, monitor the interface for failure events. In an HA configuration, an interface that has HA MON enabled and is not bound to any Failover Interface Set (FIS), is a critical interface.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Failure or disabling of any critical interface triggers HA failover. Default value: ON Possible values = ON, OFF
haheartbeat	<String>	Read-write	In a High Availability (HA) or Cluster configuration, configure the interface for sending heartbeats. In an HA or Cluster configuration, an interface that has HA Heartbeat disabled should not send the heartbeats. Default value: ON Possible values = OFF, ON
mtu	<Integer>	Read-write	The Maximum Transmission Unit (MTU) is the largest packet size, measured in bytes excluding 14 bytes ethernet header and 4 bytes CRC, that can be transmitted and received by an interface. The default value of MTU is 1500 on all the interface of Citrix ADC, some Cloud Platforms will

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			restrict Citrix ADC to use the lesser default value. Any MTU value more than 1500 is called Jumbo MTU and will make the interface as jumbo enabled. The Maximum Jumbo MTU in Citrix ADC is 9216, however, some Virtualized / Cloud Platforms will have lesser Maximum Jumbo MTU Value (9000). In the case of Cluster, the Backplane interface requires an MTU value of 78 bytes more than the Max MTU configured on any other Data-Plane Interface. When the Data plane interfaces are all at default 1500 MTU, Cluster Back Plane will be automatically set to 1578 (1500 + 78) MTU. If a Backplane interface is reset to Data Plane Interface, then the 1578 MTU will be automatically reset to the default MTU of 1500(or whatever lesser default value). If any data plane interface

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			of a Cluster is configured with a Jumbo MTU (> 1500), then all backplane interfaces require to be configured with a minimum MTU of 'Highest Data Plane MTU in the Cluster + 78'. That makes the maximum Jumbo MTU for any Data-Plane Interface in a Cluster System to be '9138 (9216 - 78)., where 9216 is the maximum Jumbo MTU. On certain Virtualized / Cloud Platforms, the maximum possible MTU is restricted to a lesser value, Similar calculation can be applied, Maximum Data Plane MTU in Cluster = (Maximum possible MTU - 78). Default value: 1500 Minimum value = 1500 Maximum value = 9216
ringsize	<Integer>	Read-write	The receive ringsize of the interface. A higher number

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			provides more number of buffers in handling incoming traffic. Default value: 2048 Minimum value = 512 Maximum value = 16384
ringtype	<String>	Read-write	The receive ringtype of the interface (Fixed or Elastic). A fixed ring type pre-allocates configured number of buffers irrespective of traffic rate. In contrast, an elastic ring, expands and shrinks based on incoming traffic rate. Default value: Elastic Possible values = Elastic, Fixed
tagall	<String>	Read-write	Add a four-byte 802.1q tag to every packet sent on this interface. The ON setting applies the tag for this interface's native VLAN. OFF applies the tag for all VLANs

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			other than the native VLAN. Default value: OFF Possible values = ON, OFF
trunk	<String>	Read-write	This argument is deprecated by tagall. Default value: OFF Possible values = ON, OFF
trunkmode	<String>	Read-write	Accept and send 802.1q VLAN tagged packets, based on Allowed Vlan List of this interface. Default value: OFF Possible values = ON, OFF
trunkallowedvlan	<String[]>	Read-write	VLAN ID or range of VLAN IDs will be allowed on this trunk interface. In the command line interface, separate the range with a hyphen. For example: 40-90. Minimum length = 1 Maximum length = 4094
lacpmode	<String>	Read-write	Bind the interface to a LA channel created by the Link

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Aggregation control protocol (LACP). Available settings function as follows: * Active - The LA channel port of the Citrix ADC generates LACPDU messages on a regular basis, regardless of any need expressed by its peer device to receive them. * Passive - The LA channel port of the Citrix ADC does not transmit LACPDU messages unless the peer device port is in the active mode. That is, the port does not speak unless spoken to. * Disabled - Unbinds the interface from the LA channel. If this is the only interface in the LA channel, the LA channel is removed.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: DISABLED Possible values = DISABLED, ACTIVE, PASSIVE
lacpkey	<Integer>	Read-write	Integer identifying the LACP LA channel to which the interface is to be bound. For an LA channel of the Citrix ADC, this digit specifies the variable x of an LA channel in LA/x notation, where x can range from 1 to 8. For example, if you specify 3 as the LACP key for an LA channel, the interface is bound to the LA channel LA/3. For an LA channel of a cluster configuration, this digit specifies the variable y of a cluster LA channel in CLA/(y-4) notation, where y can range from 5 to 8. For example, if

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			you specify 6 as the LACP key for a cluster LA channel, the interface is bound to the cluster LA channel CLA/2. Minimum value = 1 Maximum value = 8
lagtype	<String>	Read-write	Type of entity (Citrix ADC or cluster configuration) for which to create the channel. Default value: NODE Possible values = NODE, CLUSTER
lacppriority	<Integer>	Read-write	LACP port priority, expressed as an integer. The lower the number, the higher the priority. The Citrix ADC limits the number of interfaces in an LA channel to sixteen. Default value: 32768 Minimum value = 1 Maximum value = 65535

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
lacptimeout	<String>	Read-write	Interval at which the Citrix ADC sends LACPDU messages to the peer device on the LA channel. Available settings function as follows: LONG - 30 seconds. SHORT - 1 second. Default value: NSA_LACP_TIMEOUT_LONG Possible values = LONG, SHORT
ifalias	<String>	Read-write	Alias name for the interface. Used only to enhance readability. To perform any operations, you have to specify the interface ID. Default value: " " Maximum length = 31
throughput	<Integer>	Read-write	Low threshold value for the throughput of the interface, in Mbps. In an HA configuration, failover is triggered if the interface has HA MON enabled and

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			the throughput is below the specified the threshold. Minimum value = 0 Maximum value = 500000
linkredundancy	<String>	Read-write	Link Redundancy for Cluster LAG. Default value: OFF Possible values = ON, OFF
bandwidthhigh	<Integer>	Read-write	High threshold value for the bandwidth usage of the interface, in Mbps. The Citrix ADC generates an SNMP trap message when the bandwidth usage of the interface is greater than or equal to the specified high threshold value. Minimum value = 0 Maximum value = 500000
bandwidthnormal	<Integer>	Read-write	Normal threshold value for the bandwidth usage of the interface, in Mbps. When the bandwidth usage of the interface becomes less than or equal to the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			specified normal threshold after exceeding the high threshold, the Citrix ADC generates an SNMP trap message to indicate that the bandwidth usage has returned to normal. Minimum value = 0 Maximum value = 500000
lldpmode	<String>	Read-write	Link Layer Discovery Protocol (LLDP) mode for an interface. The resultant LLDP mode of an interface depends on the LLDP mode configured at the global and the interface levels. Possible values = NONE, TRANSMITTER, RECEIVER, TRANSCEIVER
lrsetpriority	<Integer>	Read-write	LRSET port priority, expressed as an integer ranging from 1 to 1024. The highest priority is 1. The Citrix ADC limits the number of interfaces in an LRSET to 8. Within a

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			LRSET the highest LR Priority Interface is considered as the first candidate for the Active interface, if the interface is UP. Default value: 1024 Minimum value = 1 Maximum value = 1024
devicename	<String>	Read-only	Name of the interface.
unit	<Integer>	Read-only	Unit number for this interface, signifying the sequence number in which this interface is discovered on this Citrix ADC.
description	<String>	Read-only	Display the type of interface, the speeds at which this interface can operate, and, if applicable, the type of SFP,.
flags	<Integer>	Read-only	Flags for this interface. Used for communicating the device states.
actualmtu	<Integer>	Read-only	MTU for this interface (the largest frame that can transit this interface).

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
vlan	<Integer>	Read-only	Native VLAN for this interface.
mac	<String>	Read-only	MAC address for this interface.
uptime	<Integer>	Read-only	Duration for which the interface has been UP (Example: 3 hours 1 minute 1 second). This value is reset when the interface state changes to DOWN..
downtime	<Integer>	Read-only	Duration for which the interface has been DOWN. This value is reset when the interface state changes to UP. (Example: 3 hours 1 minute 1 second).
actualringsize	<Integer>	Read-only	Actual receive ringsize of the interface. This will be same as configured receive ringsize when ringtype is Fixed whereas it denotes the current number of receive buffers allocated when ringtype is Elastic.
reqmedia	<String>	Read-only	Requested media setting for this interface.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = AUTO, UTP, FIBER
reqspeed	<String>	Read-only	Requested speed setting for this interface. Possible values = AUTO, 10, 100, 1000, 10000, 25000, 40000, 50000, 100000, 200000
reqduplex	<String>	Read-only	Requested duplex setting for this interface. Possible values = AUTO, HALF, FULL
reqflowcontrol	<String>	Read-only	Requested flow control setting for this interface. Possible values = OFF, RX, TX, RXTX, ON
actmedia	<String>	Read-only	Actual media setting for this interface. Possible values = AUTO, UTP, FIBER
actspeed	<String>	Read-only	Actual speed setting for this interface. Possible values = AUTO, 10, 100, 1000, 10000, 25000, 40000,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			50000, 100000, 200000
actduplex	<String>	Read-only	Actual duplex setting for this interface. Possible values = AUTO, HALF, FULL
actflowctl	<String>	Read-only	Actual flow control setting for this interface. Possible values = OFF, RX, TX, RXTX, ON
mode	<String>	Read-only	Interface Link Aggregation mode (Auto/Manual) setting. Possible values = MANUAL, AUTO
state	<String>	Read-only	Link state of the interface (UP/DOWN). Default value: ENABLED Possible values = ENABLED, DISABLED
autonegresult	<Integer>	Read-only	Actual auto-negotiation setting for this interface.
tagged	<Integer>	Read-only	VLAN tags setting on this channel.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
taggedany	<Integer>	Read-only	Interface setting to accept/drop all tagged packets.
taggedautolearn	<Integer>	Read-only	Dynamic VLAN membership autolearning enabled or disabled on this interface.
hangdetect	<Integer>	Read-only	Hang detection enabled or disabled for this interface.
hangreset	<Integer>	Read-only	Hang reset enabled or disabled for this interface.
linkstate	<Integer>	Read-only	The current state of the link associated with the interface. For logical interfaces (LA), the state of the link is dependent on the state of the slave interfaces. For the link to be UP at least one of the slave interfaces needs to be UP.
intfstate	<Integer>	Read-only	Current state of the specified interface. The interface state set to UP only if the link state is UP and administrative state is ENABLED.
rxpackets	<Integer>	Read-only	Number of packets received by an

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			interface since the Citrix ADC was started or the interface statistics were cleared.
rxbytes	<Integer>	Read-only	Number of bytes received by an interface since the Citrix ADC was started or the interface statistics were cleared.
rxerrors	<Integer>	Read-only	Number of inbound packets dropped by the hardware on a specified interface since the Citrix ADC was started or the interface statistics were cleared. Packets can be dropped because of CRC, length (undersize or oversize), or alignment errors.
rxdrops	<Integer>	Read-only	Number of inbound packets dropped by the specified interface. Commonly dropped packets are multicast frames, spanning tree BPDUs, packets destined to a MAC not owned by the Citrix ADC when L2 mode is disabled, or

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			packets tagged for a VLAN that is not bound to the interface. In most healthy networks, this statistic increments at a steady rate regardless of traffic load. A sharp spike in dropped packets generally indicates an issue with connected L2 switches, such as a forwarding database overflow resulting in packets being broadcast on all ports.
txpackets	<Integer>	Read-only	Number of packets transmitted by an interface since the Citrix ADC was started or the interface statistics were cleared.
txbytes	<Integer>	Read-only	Number of bytes transmitted by an interface since the Citrix ADC was started or the interface statistics were cleared.
txerrors	<Integer>	Read-only	Number of outbound packets dropped by the hardware on a specified interface

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			since the Citrix ADC was started or the interface statistics were cleared. Packets can be dropped because of length (undersize or oversize) errors or a lack of resources. This statistic is available only for: (1) Loop back interface (LO) of all platforms. (2) All data ports on the Citrix ADC 12000 platform. (3) Management ports on the Citrix ADC MPX 15000 and 17000 platforms. .
txdrops	<Integer>	Read-only	Number of packets dropped in transmission by the specified interface for one of the following reasons. (1) VLAN mismatch. (2) Oversized packets.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			(3) Interface congestion. (4) Loopback packets sent on non loop back interface. .
indisc	<Integer>	Read-only	Number of error-free inbound packets discarded by the specified interface because of a lack of resources (for example, insufficient receive buffers).
outdisc	<Integer>	Read-only	Number of error-free outbound packets discarded by the specified interface because of a lack of resources. This statistic is not available on: (1) 10G ports of Citrix ADC MPX 12500/12500/15500 -10G platforms. (2) 10G data ports on Citrix ADC MPX 17500/19500/21500 platforms. .
fctls	<Integer>	Read-only	Number of times flow control is performed on the specified

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			interface because of received pause frames.
hangs	<Integer>	Read-only	Number of times the specified interface detected hangs in the transmit and receive paths since the Citrix ADC was started or the interface statistics were cleared.
stsstalls	<Integer>	Read-only	Number of times the status updates for a specified interface were stalled since the Citrix ADC was started or the interface statistics were cleared. A status stall is detected when the status of the interface is not updated by the NIC hardware within 0.8 seconds of the last update.
txstalls	<Integer>	Read-only	Number of times the interface stalled, when transmitting packets, since the Citrix ADC was started or the interface statistics were cleared. Transmit (Tx) stalls are detected when a

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			packet posted for transmission is not transmitted in 4 seconds.
rxstalls	<Integer>	Read-only	Number of times the interface stalled, when receiving packets, since the Citrix ADC was started or the interface statistics were cleared. Receive (Rx) stalls are detected when the following conditions are met: (1)The link is up for more than 10 minutes. (2)Packets are transmitted, but no packets are received for 16 seconds. .
bdgmacmoved	<Integer>	Read-only	Number of MAC moves between ports. A high rate of MAC moves typically indicates a bridge loop between two interfaces.
bdgmuted	<Integer>	Read-only	Number of times the specified interface stopped transmitting and receiving

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			packets because of MAC moves between ports.
vmac	<String>	Read-only	Virtual MAC of this interface.
vmac6	<String>	Read-only	Virtual MAC for IPv6 of this interface.
reqthroughput	<Integer>	Read-only	Minimum required throughput for an interface. Failover is triggered if the operating throughput of a Link Aggregation (LA) channel for which HAMON is ON falls below this value. The possible values are: 1. 1000Mbps for 1G interfaces. 2. 10000Mbps for 10G interfaces. 3. 500000Mbps for Link Aggregation channels. Minimum value = 0 Maximum value = 500000
actthroughput	<Integer>	Read-only	Actual throughput for the interface.
backplane	<String>	Read-only	The cluster backplane status of

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			the interface. If the status is enabled, the interface is part of the cluster backplane. By default, the backplane status is disabled. Possible values = ENABLED, DISABLED
ifnum	<String[]>	Read-only	Contains the LA Master, if the interface is part of LA channel.
cleartime	<Integer>	Read-only	Time since the interface stats are cleared last time.
slavestate	<Integer>	Read-only	State of the member interfaces.
slavemedia	<Integer>	Read-only	Media type of the member interfaces.
slavespeed	<Integer>	Read-only	Speed of the member interfaces.
slaveduplex	<Integer>	Read-only	Duplex of the member interfaces.
slaveflowctl	<Integer>	Read-only	Flowcontrol of the member interfaces.
slavetime	<Integer>	Read-only	UP time of the member interfaces.
intftype	<String>	Read-only	Interface Type, this field will have the interface type either

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			it is virtual, physical or loopback. . Possible values = BROADCOM 5700/5701, TIGON1/TIGON2, INTEL 82546, INTEL 8255X(PRO), Link Aggregate, Loopback, Intel 82541/47, Broadcom 5704, Chelsio 1G, Intel 8247X, Intel 82576 VF, Xen Virtual, Intel 10G, Intel 82599 VF, Mellanox 100G, Mellanox 50G, Mellanox 25G, Intel FVL 40G, Intel FVL 25G, Intel FVL 10G, Intel FVL 40G VF, Mellanox VF, CX4 VF SMART NIC, CX3 VF, CX3 VF SMART NIC, Hyper v, Cluster LAG, Intel 8247X SFP, XEN Interface, Chelsio 10G, KVM Virtio, VMXNET3, Google Virtual NIC, Microsoft Azure MANA NIC, DPDK, Linux

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
svmcmd	<Integer>	Read-only	New attribute added to identify the source of cmd, when SVM fires the nitro cmd, it will set the value of SVMCMD to be 1. . Default value: 0
lacpactormode	<String>	Read-only	* Active - The LA channel port of the Citrix ADC generates LACPDU messages on a regular basis, regardless of any need expressed by its peer device to receive them. * Passive - The LA channel port of the Citrix ADC does not transmit LACPDU messages unless the peer device port is in the active mode. That is, the port does not speak unless spoken to. * Disabled - Unbinds the interface from the LA channel. If this is the only interface in the LA channel, the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			LA channel is removed. Possible values = DISABLED, ACTIVE, PASSIVE
lacpactortimeout	<String>	Read-only	Interval at which the Citrix ADC sends LACPDU messages to the peer device on the LA channel. Available settings function as follows: LONG - 30 seconds. SHORT - 1 second. Possible values = LONG, SHORT
lacpactorpriority	<Integer>	Read-only	LACP Actor Priority. A LACP port priority is configured on each port using LACP. LACP uses the port priority with the port number to form the port identifier. The port priority determines which ports should be put in standby mode when there is a hardware limitation that prevents all compatible ports from aggregating.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
lacpactorportno	<Integer>	Read-only	LACP Actor port number. LACP uses the port priority with the port number to form the port identifier.
lacppartnerstate	<String>	Read-only	LACP Partner State. Whether the port is in Active or Passive negotiating state. Possible values = MANUAL, AUTO
lacppartnertimeout	<String>	Read-only	The timeout value for the information revieved in LACPDUs. It can have values as SHORT or LONG. The SHORT timeout is 3s and the LONG timeout is 90s. Possible values = LONG, SHORT
lacppartneraggregation	<String>	Read-only	The Aggregation flag indicates that the participant will allow the link to be used as part of an aggregate. Otherwise the link is to be used as an individual link, i.e. not aggregated with any other. Possible values = NS_EMPTY_STR, AGG

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
lacppartnerinsync	<String>	Read-only	The Synchronization flag indicates that the transmitting participant.s mux component is in sync with the system id and key information transmitted. Possible values = NS_EMPTY_STR, SYNC
lacppartnercollecting	<String>	Read-only	The Collecting flag indicates that the participant.s collector, i.e. the reception component of the mux, is definitely on. If set the flag communicates collecting. Possible values = NS_EMPTY_STR, COLLECTING
lacppartnerdistributing	<String>	Read-only	The Distributing flag indicates that the participant.s distributor is not definitely off. If reset the flag indicates not distributing. Possible values = NS_EMPTY_STR, DISTRIBUTING
lacppartnerdefaulted	<String>	Read-only	If the timer expires in the Expired state, the Receive Machine

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			enters the Defaulted state. Possible values = NS_EMPTY_STR, DEFAULTED
lacppartnerexpired	<String>	Read-only	If the LACPDUs are received for timeout period, the Receive Machine enters the Expired state and the timer is restarted with the timeout value of SHORT timeout. Possible values = NS_EMPTY_STR, EXPIRED
lacppartnerpriority	<Integer>	Read-only	LACP Partner Priority. A LACP port priority is configured on each port using LACP. LACP uses the port priority with the port number to form the port identifier. The port priority determines which ports should be put in standby mode when there is a hardware limitation that prevents all compatible ports from aggregating.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
lacppartnersystemmac	<String>	Read-only	LACP Partner System MAC.
lacppartnersystempriority	<Integer>	Read-only	LACP Partner System Priority. The LACP partner's system priority. The values for the priority range from 0 to 65535. The lower the value, the higher the system priority. The switch with the lower system priority value determines which links between LACP partner are active and which are in the standby for each LACP Channel.
lacppartnerportno	<Integer>	Read-only	LACP Partner Port number. LACP uses the port priority with the port number to form the port identifier.
lacppartnerkey	<Integer>	Read-only	LACP Partner Key. The LACP key used by the partner port.
lacpactoraggregation	<String>	Read-only	The Aggregation flag indicates that the participant will allow the link to be used as part of an aggregate. Otherwise the link is to be used as an individual link, i.e.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			not aggregated with any other. Possible values = NS_EMPTY_STR, AGG
lacpactorinsync	<String>	Read-only	The Synchronization flag indicates that the transmitting participant.s mux component is in sync with the system id and key information transmitted. Possible values = NS_EMPTY_STR, SYNC
lacpactorcollecting	<String>	Read-only	The Collecting flag indicates that the participant.s collector, i.e. the reception component of the mux, is definitely on. If set the flag communicates collecting. Possible values = NS_EMPTY_STR, COLLECTING
lacpactordistributing	<String>	Read-only	The Distributing flag indicates that the participant.s distributor is not definitely off. If reset the flag indicates not distributing.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = NS_EMPTY_STR, DISTRIBUTING
lacpportmuxstate	<String>	Read-only	LACP Port MUX state. The state of the MUX control machine. The Mux Control Machine attaches the physical port to an aggregate port, using the Selection Logic to choose an appropriate port, and turns the distributor and collector for the physical port on or off as required by protocol information. Possible values = DETACHED, WAITING, ATTACHED, COLLECTING, DISTRIBUTING
lacpportrxstat	<String>	Read-only	LACP Port RX state. The state of the Receive machine. The Receive Machine maintains partner information, recording protocol information from LACPDUs sent by remote partner(s). Received information is subject to a timeout, and if

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			sufficient time elapses the receive machine will revert to using default partner information. Possible values = INIT, PORT_DISABLED, LACP_DISABLED, EXPIRED, DEFAULTED, CURRENT
lacpportselectstate	<String>	Read-only	LACP Port SELECT state. The state of the SELECT state machine, It could be SELECTED or UNSELECTED. Possible values = UNSELECTED, SELECTED, STANDBY
lractiveintf	<Integer>	Read-only	LR set member interface state(active/inactive).
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- CLEAR
- UPDATE
- UNSET

- ENABLE
- DISABLE
- RESET
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

CLEAR

URL: http:// <netscaler-ip-address> /nitro/v1/config/Interface? **action=clear HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"Interface":{

<b>"id":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/Interface **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"Interface":{

<b>"id":<String_value>,

</b>"speed":<String_value>,

"duplex":<String_value>,

"flowctl":<String_value>,

"autoneg":<String_value>,

"hamonitor":<String_value>,

"haheartbeat":<String_value>,
```

```
"mtu":<Integer_value>,

"ringsize":<Integer_value>,

"ringtype":<String_value>,

"tagall":<String_value>,

"trunk":<String_value>,

"trunkmode":<String_value>,

"trunkallowedvlan":<String[]_value>,

"lacpmode":<String_value>,

"lacpkey":<Integer_value>,

"lagtype":<String_value>,

"lacppriority":<Integer_value>,

"lacptimeout":<String_value>,

"ifalias":<String_value>,

"throughput":<Integer_value>,

"linkredundancy":<String_value>,

"bandwidthhigh":<Integer_value>,

"bandwidthnormal":<Integer_value>,

"lldpmode":<String_value>,

"lrsetpriority":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/Interface? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"Interface":{

<b>"id":<String_value>,

</b>"speed":true,

"duplex":true,

"flowctl":true,

"autoneg":true,

"hamonitor":true,

"haheartbeat":true,

"mtu":true,

"ringsize":true,

"ringtype":true,

"tagall":true,

"trunk":true,

"trunkmode":true,

"trunkallowedvlan":true,
```

```
"lacpmode":true,

"lacppriority":true,

"lacptimeout":true,

"ifalias":true,

"throughput":true,

"linkredundancy":true,

"bandwidthhigh":true,

"bandwidthnormal":true,

"lldpmode":true,

"lrsetpriority":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

ENABLE

URL: http:// <netscaler-ip-address> /nitro/v1/config/Interface? **action=enable HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"Interface":{

<b>"id":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DISABLE

URL: http:// <netscaler-ip-address> /nitro/v1/config/Interface? **action=disable HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"Interface":{

<b>"id":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

RESET

URL: http:// <netscaler-ip-address> /nitro/v1/config/Interface? **action=reset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"Interface":{

<b>"id":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/Interface **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/Interface? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/Interface? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of Interface resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/Interface? **view=summary**

Use this query-parameter to get the summary output of Interface resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/Interface? **pagesize=#no;pageno=#no**

Use this query-parameter to get the Interface resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "Interface": [ {

"id":<String_value>,

"devicename":<String_value>,

"unit":<Integer_value>,

"description":<String_value>,

"flags":<Integer_value>,

"mtu":<Integer_value>,

"actualmtu":<Integer_value>,

"vlan":<Integer_value>,

"mac":<String_value>,

"uptime":<Integer_value>,

"downtime":<Integer_value>,

"ringsize":<Integer_value>,

"ringtype":<String_value>,

"actualringsize":<Integer_value>,

"reqmedia":<String_value>,
```

```
"reqspeed":<String_value>,

"reqduplex":<String_value>,

"reqflowcontrol":<String_value>,

"actmedia":<String_value>,

"actspeed":<String_value>,

"actduplex":<String_value>,

"actflowctl":<String_value>,

"mode":<String_value>,

"hamonitor":<String_value>,

"haheartbeat":<String_value>,

"state":<String_value>,

"autoneg":<String_value>,

"autonegresult":<Integer_value>,

"tagged":<Integer_value>,

"tagall":<String_value>,

"trunk":<String_value>,

"trunkmode":<String_value>,

"trunkallowedvlan":<String[]_value>,

"taggedany":<Integer_value>,

"taggedautolearn":<Integer_value>,

"hangdetect":<Integer_value>,

"hangreset":<Integer_value>,
```

```
"linkstate":<Integer_value>,

"intfstate":<Integer_value>,

"rxpackets":<Integer_value>,

"rxbytes":<Integer_value>,

"rxerrors":<Integer_value>,

"rxdrops":<Integer_value>,

"txpackets":<Integer_value>,

"txbytes":<Integer_value>,

"txerrors":<Integer_value>,

"txdrops":<Integer_value>,

"indisc":<Integer_value>,

"outdisc":<Integer_value>,

"fctls":<Integer_value>,

"hangs":<Integer_value>,

"stsstalls":<Integer_value>,

"txstalls":<Integer_value>,

"rxstalls":<Integer_value>,

"bdgmacmoved":<Integer_value>,

"bdgmuted":<Integer_value>,

"vmac":<String_value>,

"vmac6":<String_value>,

"lacpmode":<String_value>,
```

```
"lacpkey":<Integer_value>,

"lacppriority":<Integer_value>,

"lacptimeout":<String_value>,

"lagtype":<String_value>,

"ifalias":<String_value>,

"reqthroughput":<Integer_value>,

"linkredundancy":<String_value>,

"actthroughput":<Integer_value>,

"bandwidthhigh":<Integer_value>,

"bandwidthnormal":<Integer_value>,

"backplane":<String_value>,

"ifnum":<String[]_value>,

"cleartime":<Integer_value>,

"slavestate":<Integer_value>,

"slavemedia":<Integer_value>,

"slavespeed":<Integer_value>,

"slaveduplex":<Integer_value>,

"slaveflowctl":<Integer_value>,

"slavetime":<Integer_value>,

"intftype":<String_value>,

"svmcmd":<Integer_value>,

"lacpactormode":<String_value>,
```

```
"lacpactortimeout":<String_value>,

"lacpactorpriority":<Integer_value>,

"lacpactorportno":<Integer_value>,

"lacppartnerstate":<String_value>,

"lacppartnertimeout":<String_value>,

"lacppartneraggregation":<String_value>,

"lacppartnerinsync":<String_value>,

"lacppartnercollecting":<String_value>,

"lacppartnerdistributing":<String_value>,

"lacppartnerdefaulted":<String_value>,

"lacppartnerexpired":<String_value>,

"lacppartnerpriority":<Integer_value>,

"lacppartnersystemmac":<String_value>,

"lacppartnersystempriority":<Integer_value>,

"lacppartnerportno":<Integer_value>,

"lacppartnerkey":<Integer_value>,

"lacpactoraggregation":<String_value>,

"lacpactorinsync":<String_value>,

"lacpactorcollecting":<String_value>,

"lacpactordistributing":<String_value>,

"lacpportmuxstate":<String_value>,

"lacpportrxstat":<String_value>,
```

```
"lacpportselectstate":<String_value>,

"lldpmode":<String_value>,

"lrsetpriority":<Integer_value>,

"lractiveintf":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/Interface/ id_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/Interface/ id_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/Interface/ id_value<String> ? **view=summary**

Use this query-parameter to get the summary output of Interface resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "Interface": [ {

"id":<String_value>,

"devicename":<String_value>,

"unit":<Integer_value>,

"description":<String_value>,

"flags":<Integer_value>,

"mtu":<Integer_value>,

"actualmtu":<Integer_value>,

"vlan":<Integer_value>,

"mac":<String_value>,

"uptime":<Integer_value>,

"downtime":<Integer_value>,

"ringsize":<Integer_value>,

"ringtype":<String_value>,

"actualringsize":<Integer_value>,

"reqmedia":<String_value>,

"reqspeed":<String_value>,

"reqduplex":<String_value>,

"reqflowcontrol":<String_value>,

"actmedia":<String_value>,

"actspeed":<String_value>,
```

```
"actduplex":<String_value>,

"actflowctl":<String_value>,

"mode":<String_value>,

"hamonitor":<String_value>,

"haheartbeat":<String_value>,

"state":<String_value>,

"autoneg":<String_value>,

"autonegresult":<Integer_value>,

"tagged":<Integer_value>,

"tagall":<String_value>,

"trunk":<String_value>,

"trunkmode":<String_value>,

"trunkallowedvlan":<String[]_value>,

"taggedany":<Integer_value>,

"taggedautolearn":<Integer_value>,

"hangdetect":<Integer_value>,

"hangreset":<Integer_value>,

"linkstate":<Integer_value>,

"intfstate":<Integer_value>,

"rxpackets":<Integer_value>,

"rxbytes":<Integer_value>,

"rxerrors":<Integer_value>,
```

```
"rxdrops":<Integer_value>,

"txpackets":<Integer_value>,

"txbytes":<Integer_value>,

"txerrors":<Integer_value>,

"txdrops":<Integer_value>,

"indisc":<Integer_value>,

"outdisc":<Integer_value>,

"fctls":<Integer_value>,

"hangs":<Integer_value>,

"stsstalls":<Integer_value>,

"txstalls":<Integer_value>,

"rxstalls":<Integer_value>,

"bdgmacmoved":<Integer_value>,

"bdgmuted":<Integer_value>,

"vmac":<String_value>,

"vmac6":<String_value>,

"lacpmode":<String_value>,

"lacpkey":<Integer_value>,

"lacppriority":<Integer_value>,

"lacptimeout":<String_value>,

"lagtype":<String_value>,

"ifalias":<String_value>,
```

```
"reqthroughput":<Integer_value>,

"linkredundancy":<String_value>,

"actthroughput":<Integer_value>,

"bandwidthhigh":<Integer_value>,

"bandwidthnormal":<Integer_value>,

"backplane":<String_value>,

"ifnum":<String[]_value>,

"cleartime":<Integer_value>,

"slavestate":<Integer_value>,

"slavemedia":<Integer_value>,

"slavespeed":<Integer_value>,

"slaveduplex":<Integer_value>,

"slaveflowctl":<Integer_value>,

"slavetime":<Integer_value>,

"intftype":<String_value>,

"svmcmd":<Integer_value>,

"lacpactormode":<String_value>,

"lacpactortimeout":<String_value>,

"lacpactorpriority":<Integer_value>,

"lacpactorportno":<Integer_value>,

"lacppartnerstate":<String_value>,

"lacppartnertimeout":<String_value>,
```

```
"lacppartneraggregation":<String_value>,

"lacppartnerinsync":<String_value>,

"lacppartnercollecting":<String_value>,

"lacppartnerdistributing":<String_value>,

"lacppartnerdefaulted":<String_value>,

"lacppartnerexpired":<String_value>,

"lacppartnerpriority":<Integer_value>,

"lacppartnersystemmac":<String_value>,

"lacppartnersystempriority":<Integer_value>,

"lacppartnerportno":<Integer_value>,

"lacppartnerkey":<Integer_value>,

"lacpactoraggregation":<String_value>,

"lacpactorinsync":<String_value>,

"lacpactorcollecting":<String_value>,

"lacpactordistributing":<String_value>,

"lacpportmuxstate":<String_value>,

"lacpportrxstat":<String_value>,

"lacpportselectstate":<String_value>,

"lldpmode":<String_value>,

"lrsetpriority":<Integer_value>,

"lractiveintf":<Integer_value>,

"_nextgenapiresource":<String_value>
```

```
}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/Interface? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "Interface": [ { "__count": "#no"} ] }
```

appalgparam

Configuration for AppAlg Param resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
pptpgreidletimeout	<Integer>	Read-write	Interval in sec, after which data sessions of PPTP GRE is cleared. Default value: 9000

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum value = 1 Maximum value = 9000
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- UPDATE
- UNSET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/appalgparam **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"appalgparam":{

"pptpgreidletimeout":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/appalgparam? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"appalgparam":{

"pptpgreidletimeout":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/appalgparam **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "appalgparam": [ {

"pptpgreidletimeout":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

arp

Configuration for arp resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ipaddress	<String>	Read-write	IP address of the network device that you want to add to the ARP table. Minimum length = 1
td	<Integer>	Read-write	Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0. Minimum value = 0 Maximum value = 4094
mac	<String>	Read-write	MAC address of the network device.
ifnum	<String>	Read-write	Interface through which the network device is accessible. Specify the interface in (slot/port) notation. For example, 1/3.
vxlan	<Integer>	Read-write	ID of the VXLAN on which the IP address of this ARP entry is reachable. Minimum value = 1 Maximum value = 16777215

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
vtep	<String>	Read-write	IP address of the VXLAN tunnel endpoint (VTEP) through which the IP address of this ARP entry is reachable. Minimum length = 1
vlan	<Integer>	Read-write	The VLAN ID through which packets are to be sent after matching the ARP entry. This is a numeric value.
ownernode	<Integer>	Read-write	The owner node for the Arp entry. Minimum value = 0 Maximum value = 31
all	<Boolean>	Read-write	Remove all ARP entries from the ARP table of the Citrix ADC.
nodeid	<Integer>	Read-write	Unique number that identifies the cluster node. Minimum value = 0 Maximum value = 31
timeout	<Integer>	Read-only	The time, in seconds, after which the entry times out.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
state	<Integer>	Read-only	The state of the ARP entry.
flags	<Integer>	Read-only	The flags for the entry.
type	<String>	Read-only	Indicates whether this ARP entry was added manually or dynamically. When you manually add an ARP entry, the value for this parameter is STATIC. Otherwise, it is DYNAMIC. For the NSIP and loopback IP addresses, the value is PERMANENT. Possible values = STATIC, PERMANENT, DYNAMIC
channel	<Integer>	Read-only	The tunnel, channel, or physical interface through which the ARP entry is identified.
controlplane	<Boolean>	Read-only	This arp entry is populated by a control plane protocol.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- SEND
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/arp **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"arp":{

<b>"ipaddress":<String_value>,

</b>"td":<Integer_value>,

<b>"mac":<String_value>,

</b>"ifnum":<String_value>,

"vxlan":<Integer_value>,

"vtep":<String_value>,

"vlan":<Integer_value>,

"ownernode":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/arp/ ipaddress_value<String> **Query-parameters: args=td: <Integer_value> ,all: <Boolean_value> ,ownernode: <Integer_value>**
send
URL: http:// <netscaler-ip-address> /nitro/v1/config/arp? **action=send HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"arp":{

"ipaddress":<String_value>,

"td":<Integer_value>,

"all":<Boolean_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error
get (all)
URL: http:// <netscaler-ip-address> /nitro/v1/config/arp **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/arp? **args=ipaddress: <String_value> ,td: <Integer_value> ,ownernode: <Integer_value> ,nodeid: <Integer_value>**

Use this query-parameter to get arp resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/config/arp? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/arp? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of arp resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/arp? **view=summary**

Use this query-parameter to get the summary output of arp resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/arp? **pagesize=#no;pageno=#no**

Use this query-parameter to get the arp resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "arp": [ {

ipaddress:<String_value>,td:<Integer_value>,ownernode:<Integer_value>,node
id:<Integer_value>"mac":<String_value>,

"ifnum":<String_value>,

"timeout":<Integer_value>,

"state":<Integer_value>,

"flags":<Integer_value>,

"type":<String_value>,

"vlan":<Integer_value>,

"vxlan":<Integer_value>,

"vtep":<String_value>,

"channel":<Integer_value>,

"controlplane":<Boolean_value>,
```

```
"_nextgenapiresource":<String_value>

}]}
```

count

URL: http:// <netscaler-ip-address> /nitro/v1/config/arp? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "arp": [ { "__count": "#no"} ] }
```

arpparam

Configuration for Global arp parameters resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
timeout	<Integer>	Read-write	Time-out value (aging time) for the dynamically learned ARP entries, in seconds. The new

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			value applies only to ARP entries that are dynamically learned after the new value is set. Previously existing ARP entries expire after the previously configured aging time. Default value: 1200 Minimum value = 5 Maximum value = 1200
spoofvalidation	<String>	Read-write	enable/disable arp spoofing validation. Default value: DISABLED Possible values = ENABLED, DISABLED
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- UPDATE
- UNSET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/arpparam **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"arpparam":{

"timeout":<Integer_value>,

"spoofvalidation":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/arpparam? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"arpparam":{

"timeout":true,

"spoofvalidation":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/arpparam **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "arpparam": [ {

"timeout":<Integer_value>,

"spoofvalidation":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

bridgegroup

Configuration for bridge group resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
id	<Integer>	Read-write	An integer that uniquely identifies the bridge group. Minimum value = 1 Maximum value = 1000
dynamicrouting	<String>	Read-write	Enable dynamic routing for this bridgegroup. Default value: DISABLED Possible values = ENABLED, DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ipv6dynamicrouting	<String>	Read-write	Enable all IPv6 dynamic routing protocols on all VLANs bound to this bridgegroup. Note: For the ENABLED setting to work, you must configure IPv6 dynamic routing protocols from the VTYSH command line. Default value: DISABLED Possible values = ENABLED, DISABLED
flags	<Boolean>	Read-only	Temporary flag used for internal purpose.
portbitmap	<Integer>	Read-only	Member interfaces of this bridge group.
tagbitmap	<Integer>	Read-only	Tagged members of this bridge group.
ifaces	<String>	Read-only	Names of all member interfaces of this bridge group.
tagifaces	<String>	Read-only	Names of all tagged member interfaces of this bridge group.
rnat	<Boolean>	Read-only	Temporary flag used for internal purpose.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
partitionname	<String>	Read-only	Name of the Partition to which this vlan bound to. Minimum length = 1
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/bridgegroup **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"bridgegroup":{

<b>"id":<Integer_value>,

</b>"dynamicrouting":<String_value>,

"ipv6dynamicrouting":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/bridgegroup/ id_value<Integer> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/bridgegroup **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"bridgegroup":{

<b>"id":<Integer_value>,

</b>"dynamicrouting":<String_value>,

"ipv6dynamicrouting":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/bridgegroup? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"bridgegroup":{

<b>"id":<Integer_value>,

</b>"dynamicrouting":true,

"ipv6dynamicrouting":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/bridgegroup **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/bridgegroup? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/bridgegroup? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of bridgegroup resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/bridgegroup? **view=summary**

Use this query-parameter to get the summary output of bridgegroup resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/bridgegroup? **pagesize=#no;pageno=#no**

Use this query-parameter to get the bridgegroup resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "bridgegroup": [ {

"id":<Integer_value>,

"flags":<Boolean_value>,

"portbitmap":<Integer_value>,

"tagbitmap":<Integer_value>,

"ifaces":<String_value>,

"tagifaces":<String_value>,

"dynamicrouting":<String_value>,

"ipv6dynamicrouting":<String_value>,

"rnat":<Boolean_value>,

"partitionname":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/bridgegroup/ id_value<Integer> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/bridgegroup/ id_value<Integer> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/bridgegroup/ id_value<Integer> ? **view=summary**

Use this query-parameter to get the summary output of bridgegroup resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "bridgegroup": [ {

"id":<Integer_value>,

"flags":<Boolean_value>,

"portbitmap":<Integer_value>,

"tagbitmap":<Integer_value>,
```

```
"ifaces":<String_value>,

"tagifaces":<String_value>,

"dynamicrouting":<String_value>,

"ipv6dynamicrouting":<String_value>,

"rnat":<Boolean_value>,

"partitionname":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/bridgegroup? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "bridgegroup": [ { "__count": "#no"} ] }
```

bridgegroup_binding

Binding object which returns the resources bound to bridgegroup.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
id	<Integer>	Read-write	The name of the bridge group. Minimum value = 1 Maximum value = 1000
bridgegroup_nsip_binding	<bridgegroup_nsip_binding[]>	Read-only	nsip that can be bound to bridgegroup.
bridgegroup_nsip6_binding	<bridgegroup_nsip6_binding[]>	Read-only	nsip6 that can be bound to bridgegroup.
bridgegroup_vlan_binding	<bridgegroup_vlan_binding[]>	Read-only	vlan that can be bound to bridgegroup.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/bridgegroup_binding/ id_value<Integer> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "bridgegroup_binding": [ {

"id":<Integer_value>,

"bridgegroup_nsip6_binding":<bridgegroup_nsip6_binding[]_value>,
```

```
"bridgegroup_vlan_binding":<bridgegroup_vlan_binding[]_value>,

"bridgegroup_nsip_binding":<bridgegroup_nsip_binding[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/bridgegroup_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/bridgegroup_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "bridgegroup_binding": [ {

"id":<Integer_value>,

"bridgegroup_nsip6_binding":<bridgegroup_nsip6_binding[]_value>,

"bridgegroup_vlan_binding":<bridgegroup_vlan_binding[]_value>,

"bridgegroup_nsip_binding":<bridgegroup_nsip_binding[]_value>
```

```
}]}
```

bridgegroup_nsip6_binding

Binding object showing the nsip6 that can be bound to bridgegroup.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
netmask	<String>	Read-write	A subnet mask associated with the network address. Minimum length = 1
ipaddress	<String>	Read-write	The IP address assigned to the bridge group.
ownergroup	<String>	Read-write	The owner node group in a Cluster for this vlan. Default value: DEFAULT_NG Minimum length = 1
id	<Integer>	Read-write	The integer that uniquely identifies the bridge group. Minimum value = 1 Maximum value = 1000
td	<Integer>	Read-write	Integer value that uniquely identifies the traffic domain in which you want to configure the entity.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0. Minimum value = 0 Maximum value = 4094
rnat	<Boolean>	Read-only	Temporary flag used for internal purpose.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of

creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/bridgegroup_nsip6_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"bridgegroup_nsip6_binding":{

<b>"id":<Integer_value>,

</b>"ipaddress":<String_value>,

"netmask":<String_value>,

"td":<Integer_value>,

"ownergroup":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/bridgegroup_nsip6_binding/ id_value<Integer> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/bridgegroup_nsip6_binding/ id_value<Integer> ? **args=ipaddress: <String_value> ,netmask: <String_value> ,td: <Integer_value> ,ownergroup: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/bridgegroup_nsip6_binding/ id_value<Integer> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/bridgegroup_nsip6_binding/ id_value<Integer> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of bridgegroup_nsip6_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/bridgegroup_nsip6_binding/ id_value<Integer> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the bridgegroup_nsip6_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "bridgegroup_nsip6_binding": [ {

"netmask":<String_value>,

"ipaddress":<String_value>,

"ownergroup":<String_value>,

"id":<Integer_value>,

"td":<Integer_value>,

"rnat":<Boolean_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/bridgegroup_nsip6_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/bridgegroup_nsip6_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "bridgegroup_nsip6_binding": [ {

"netmask":<String_value>,

"ipaddress":<String_value>,

"ownergroup":<String_value>,

"id":<Integer_value>,

"td":<Integer_value>,

"rnat":<Boolean_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/bridgegroup_nsip6_binding/ id_value<Integer> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"bridgegroup_nsip6_binding": [ { "__count": "#no"} ] }
```

bridgegroup_nsip_binding

Binding object showing the nsip that can be bound to bridgegroup.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ipaddress	<String>	Read-write	The IP address assigned to the bridge group.
td	<Integer>	Read-write	Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0. Minimum value = 0 Maximum value = 4094
ownergroup	<String>	Read-write	The owner node group in a Cluster for this vlan. Default value: DEFAULT_NG

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum length = 1
id	<Integer>	Read-write	The integer that uniquely identifies the bridge group. Minimum value = 1 Maximum value = 1000
netmask	<String>	Read-write	The network mask for the subnet defined for the bridge group.
rnat	<Boolean>	Read-only	Temporary flag used for internal purpose.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/bridgegroup_nsip_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"bridgegroup_nsip_binding":{

<b>"id":<Integer_value>,

</b>"ipaddress":<String_value>,

"netmask":<String_value>,

"td":<Integer_value>,

"ownergroup":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/bridgegroup_nsip_binding/ id_value<Integer> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/bridgegroup_nsip_binding/ id_value<Integer> ? **args=ipaddress: <String_value> ,netmask: <String_value> ,td: <Integer_value> ,ownergroup: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/bridgegroup_nsip_binding/ id_value<Integer> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/bridgegroup_nsip_binding/ id_value<Integer> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of bridgegroup_nsip_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/bridgegroup_nsip_binding/ id_value<Integer> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the bridgegroup_nsip_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "bridgegroup_nsip_binding": [ {

"ipaddress":<String_value>,

"td":<Integer_value>,

"ownergroup":<String_value>,

"id":<Integer_value>,

"netmask":<String_value>,

"rnat":<Boolean_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/bridgegroup_nsip_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/bridgegroup_nsip_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "bridgegroup_nsip_binding": [ {

"ipaddress":<String_value>,

"td":<Integer_value>,

"ownergroup":<String_value>,

"id":<Integer_value>,

"netmask":<String_value>,

"rnat":<Boolean_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/bridgegroup_nsip_binding/ id_value<Integer> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"bridgegroup_nsip_binding": [ { "__count": "#no"} ] }
```

bridgegroup_vlan_binding

Binding object showing the vlan that can be bound to bridgegroup.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
vlan	<Integer>	Read-write	Names of all member VLANs.
id	<Integer>	Read-write	The integer that uniquely identifies the bridge group. Minimum value = 1 Maximum value = 1000
rnat	<Boolean>	Read-only	Temporary flag used for internal purpose.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/bridgegroup_vlan_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"bridgegroup_vlan_binding":{

<b>"id":<Integer_value>,
```

```
</b>"vlan":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/bridgegroup_vlan_binding/ id_value<Integer> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/bridgegroup_vlan_binding/ id_value<Integer> ? **args=vlan: <Integer_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/bridgegroup_vlan_binding/ id_value<Integer> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/bridgegroup_vlan_binding/ id_value<Integer> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of bridgegroup_vlan_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/bridgegroup_vlan_binding/ id_value<Integer> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the bridgegroup_vlan_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "bridgegroup_vlan_binding": [ {

"vlan":<Integer_value>,

"id":<Integer_value>,

"rnat":<Boolean_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/bridgegroup_vlan_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/bridgegroup_vlan_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "bridgegroup_vlan_binding": [ {

"vlan":<Integer_value>,

"id":<Integer_value>,

"rnat":<Boolean_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/bridgegroup_vlan_binding/ id_value<Integer> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"bridgegroup_vlan_binding": [ { "__count": "#no"} ] }
```

bridgetable

Configuration for bridge table entry resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
mac	<String>	Read-write	The MAC address of the target.
vxlan	<Integer>	Read-write	The VXLAN to which this address is associated. Minimum value = 1 Maximum value = 16777215
vtep	<String>	Read-write	The IP address of the destination VXLAN tunnel endpoint where the Ethernet MAC ADDRESS resides. Minimum length = 1
vni	<Integer>	Read-write	The VXLAN VNI Network Identifier (or VXLAN Segment ID) to use to connect to the remote VXLAN tunnel endpoint. If omitted the value specified as vxlan will be used. Minimum value = 1 Maximum value = 16777215

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
devicevlan	<Integer>	Read-write	The vlan on which to send multicast packets when the VXLAN tunnel endpoint is a muticast group address. Minimum value = 1 Maximum value = 4094
bridgeage	<Integer>	Read-write	Time-out value for the bridge table entries, in seconds. The new value applies only to the entries that are dynamically learned after the new value is set. Previously existing bridge table entries expire after the previously configured time-out value. Default value: 300 Minimum value = 60 Maximum value = 300
nodeid	<Integer>	Read-write	Unique number that identifies the cluster node. Minimum value = 0 Maximum value = 31

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
vlan	<Integer>	Read-write	VLAN whose entries are to be removed. Minimum value = 1 Maximum value = 4094
ifnum	<String>	Read-write	INTERFACE whose entries are to be removed.
flags	<Integer>	Read-only	Display flags,.
type	<String>	Read-only	Whether static or dynamic. Possible values = STATIC, PERMANENT, DYNAMIC
channel	<Integer>	Read-only	The Tunnel through which bridge entry is learned.
controlplane	<Boolean>	Read-only	This bridge table entry is populated by a control plane protocol.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE

- UNSET
- GET (ALL)
- COUNT
- CLEAR

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/bridgetable **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"bridgetable":{

<b>"mac":<String_value>,

</b><b>"vxlan":<Integer_value>,

</b><b>"vtep":<String_value>,

</b>"vni":<Integer_value>,

"devicevlan":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/bridgetable **Query-parameters: args= mac:<String_value>, vxlan:<Integer_value>, vtep: <String_value> ,devicevlan: <Integer_value>**
update
URL: http:// <netscaler-ip-address> /nitro/v1/config/bridgetable **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"bridgetable":{

"bridgeage":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

unset

URL: http:// <netscaler-ip-address> /nitro/v1/config/bridgetable? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"bridgetable":{

"bridgeage":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

clear

URL: http:// <netscaler-ip-address> /nitro/v1/config/bridgetable? **action=clear HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"bridgetable":{

"vlan":<Integer_value>,
```

```
"ifnum":<String_value>,

"vxlan":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error
get (all)
URL: http:// <netscaler-ip-address> /nitro/v1/config/bridgetable **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/bridgetable? **args=nodeid: <Integer_value>**

Use this query-parameter to get bridgetable resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/config/bridgetable? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/bridgetable? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of bridgetable resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/bridgetable? **view=summary**

Use this query-parameter to get the summary output of bridgetable resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/bridgetable? **pagesize=#no;pageno=#no**

Use this query-parameter to get the bridgetable resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "bridgetable": [ {

nodeid:<Integer_value>"bridgeage":<Integer_value>,

"mac":<String_value>,

"ifnum":<String_value>,

"vlan":<Integer_value>,

"vxlan":<Integer_value>,

"vtep":<String_value>,

"vni":<Integer_value>,

"devicevlan":<Integer_value>,

"flags":<Integer_value>,

"type":<String_value>,

"channel":<Integer_value>,

"controlplane":<Boolean_value>,

"_nextgenapiresource":<String_value>

}]}
```

count

URL: http:// <netscaler-ip-address> /nitro/v1/config/bridgetable? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "bridgetable": [ { "__count": "#no"} ] }
```

channel

Configuration for channel resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
id	<String>	Read-write	ID for the LA channel or cluster LA channel or LR channel to be created. Specify an LA channel in LA/x notation, where x can range from 1 to 8 or cluster LA channel in CLA/x

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			notation or Link redundant channel in LR/x notation, where x can range from 1 to 4. Cannot be changed after the LA channel is created.
ifnum	<String[]>	Read-write	Interfaces to be bound to the LA channel of a Citrix ADC or to the LA channel of a cluster configuration. For an LA channel of a Citrix ADC, specify an interface in C/U notation (for example, 1/3). For an LA channel of a cluster configuration, specify an interface in N/C/U notation (for example, 2/1/3). where C can take one of the following values: * 0 - Indicates a management interface. * 1 - Indicates a 1 Gbps port.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			* 10 - Indicates a 10 Gbps port. U is a unique integer for representing an interface in a particular port group. N is the ID of the node to which an interface belongs in a cluster configuration. Use spaces to separate multiple entries.
state	<String>	Read-write	Enable or disable the LA channel. Default value: ENABLED Possible values = ENABLED, DISABLED
mode	<String>	Read-write	The initital mode for the LA channel. Possible values = MANUAL, AUTO
conndistr	<String>	Read-write	The 'connection' distribution mode for the LA channel.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = DISABLED, ENABLED
macdistr	<String>	Read-write	The 'MAC' distribution mode for the LA channel. Possible values = SOURCE, DESTINATION, BOTH
lamac	<String>	Read-write	Specifies a MAC address for the LA channels configured in Citrix ADC virtual appliances (VPX). This MAC address is persistent after each reboot. If you don't specify this parameter, a MAC address is generated randomly for each LA channel. These MAC addresses change after each reboot.
speed	<String>	Read-write	Ethernet speed of the channel, in Mbps. If the speed of any bound interface is greater than or equal to the value set for this parameter, the state of the interface is UP.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Otherwise, the state is INACTIVE. Bound Interfaces whose state is INACTIVE do not process any traffic. Default value: AUTO Possible values = AUTO, 10, 100, 1000, 10000, 25000, 40000, 50000, 100000, 200000
flowctl	<String>	Read-write	Specifies the flow control type for this LA channel to manage the flow of frames. Flow control is a function as mentioned in clause 31 of the IEEE 802.3 standard. Flow control allows congested ports to pause traffic from the peer device. Flow control is achieved by sending PAUSE frames. Default value: OFF Possible values = OFF, RX, TX, RXTX, ON
hamonitor	<String>	Read-write	In a High Availability (HA) configuration,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			monitor the LA channel for failure events. Failure of any LA channel that has HA MON enabled triggers HA failover. Default value: ON Possible values = ON, OFF
haheartbeat	<String>	Read-write	In a High Availability (HA) configuration, configure the LA channel for sending heartbeats. LA channel that has HA Heartbeat disabled should not send the heartbeats. Default value: ON Possible values = OFF, ON
tagall	<String>	Read-write	Adds a four-byte 802.1q tag to every packet sent on this channel. The ON setting applies tags for all VLANs that are bound to this channel. OFF applies the tag for all VLANs other than the native VLAN. Default value: OFF

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ON, OFF
trunk	<String>	Read-write	This is deprecated by tagall. Default value: OFF Possible values = ON, OFF
ifalias	<String>	Read-write	Alias name for the LA channel. Used only to enhance readability. To perform any operations, you have to specify the LA channel ID. Default value: " " Maximum length = 31
throughput	<Integer>	Read-write	Low threshold value for the throughput of the LA channel, in Mbps. In an high availability (HA) configuration, failover is triggered when the LA channel has HA MON enabled and the throughput is below the specified threshold. Minimum value = 0 Maximum value = 500000

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
bandwidthhigh	<Integer>	Read-write	High threshold value for the bandwidth usage of the LA channel, in Mbps. The Citrix ADC generates an SNMP trap message when the bandwidth usage of the LA channel is greater than or equal to the specified high threshold value. Minimum value = 0 Maximum value = 500000
bandwidthnormal	<Integer>	Read-write	Normal threshold value for the bandwidth usage of the LA channel, in Mbps. When the bandwidth usage of the LA channel returns to less than or equal to the specified normal threshold after exceeding the high threshold, the Citrix ADC generates an SNMP trap message to indicate that the bandwidth usage has returned to normal. Minimum value = 0 Maximum value = 500000

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
mtu	<Integer>	Read-write	The Maximum Transmission Unit (MTU) is the largest packet size, measured in bytes excluding 14 bytes ethernet header and 4 bytes CRC, that can be transmitted and received by an interface. The default value of MTU is 1500 on all the interface of Citrix ADC, some Cloud Platforms will restrict Citrix ADC to use the lesser default value. Any MTU value more than 1500 is called Jumbo MTU and will make the interface as jumbo enabled. The Maximum Jumbo MTU in Citrix ADC is 9216, however, some Virtualized / Cloud Platforms will have lesser Maximum Jumbo MTU Value (9000). In the case of Cluster, the Backplane interface requires an MTU value of 78 bytes more than the Max MTU configured on any other Data-Plane Interface. When the Data plane interfaces

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			are all at default 1500 MTU, Cluster Back Plane will be automatically set to 1578 (1500 + 78) MTU. If a Backplane interface is reset to Data Plane Interface, then the 1578 MTU will be automatically reset to the default MTU of 1500(or whatever lesser default value). If any data plane interface of a Cluster is configured with a Jumbo MTU (> 1500), then all backplane interfaces require to be configured with a minimum MTU of 'Highest Data Plane MTU in the Cluster + 78'. That makes the maximum Jumbo MTU for any Data-Plane Interface in a Cluster System to be '9138 (9216 - 78)., where 9216 is the maximum Jumbo MTU. On certain Virtualized / Cloud Platforms, the maximum possible MTU is restricted to a lesser value, Similar calculation can be applied,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum Data Plane MTU in Cluster = (Maximum possible MTU - 78). . Default value: 1500 Minimum value = 1500 Maximum value = 9216
lrminthroughput	<Integer>	Read-write	Specifies the minimum throughput threshold (in Mbps) to be met by the active subchannel. Setting this parameter automatically divides an LACP channel into logical subchannels, with one subchannel active and the others in standby mode. When the maximum supported throughput of the active channel falls below the lrMinThroughput value, link failover occurs and a standby subchannel becomes active. Minimum value = 0 Maximum value = 80000

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
linkredundancy	<String>	Read-write	Link Redundancy for Cluster LAG. Default value: OFF Possible values = ON, OFF
devicename	<String>	Read-only	LA channel name in form LA/x, where x is channel ID, which ranges from 1 to 8 or LR channel name in form LR/x, where x is channel ID, which ranges from 1 to 4.
unit	<Integer>	Read-only	Unit number of the channel. This is an internal reference number that the Citrix ADC uses to identify the channel.
description	<String>	Read-only	The IEEE standard that the channel is based on.
flags	<Integer>	Read-only	Flags of this channel.
actualmtu	<Integer>	Read-only	MTU of the channel. This is the maximum frame size that the channel can process.
vlan	<Integer>	Read-only	Native VLAN of the channel.
mac	<String>	Read-only	MAC address of the channel.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
uptime	<Integer>	Read-only	Duration for which the channel is UP. (Example: 3 hours 1 minute 1 second). This value is reset when the channel state changes to DOWN.
downtime	<Integer>	Read-only	Duration for which the channel is DOWN. (Example: 3 hours 1 minute 1 second). This value is reset when the channel state changes to UP.
reqmedia	<String>	Read-only	Requested media setting for this channel. Since there is no media associated with LA, the displayed values carry no significance. Possible values = AUTO, UTP, FIBER
reqspeed	<String>	Read-only	Requested speed setting for this channel. Since no media are associated with LA, this speed is used to determine the threshold for the slave interfaces. If the speed of the member interface is less than the requested speed,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			that interface is considered inactive. Possible values = AUTO, 10, 100, 1000, 10000, 25000, 40000, 50000, 100000, 200000
reqduplex	<String>	Read-only	Requested duplex setting for this channel. Since no media are associated with LA, the displayed values carry no significance. Possible values = AUTO, HALF, FULL
reqflowcontrol	<String>	Read-only	Requested flow control setting for this channel. Since no media are associated with LA, the displayed values carry no significance. Possible values = OFF, RX, TX, RXTX, ON
media	<String>	Read-only	Requested media setting for this interface. Possible values = AUTO, UTP, FIBER
actspeed	<String>	Read-only	Actual speed setting for this channel.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = AUTO, 10, 100, 1000, 10000, 25000, 40000, 50000, 100000, 200000
duplex	<String>	Read-only	Actualduplex setting for this interface. Possible values = AUTO, HALF, FULL
actflowctl	<String>	Read-only	Actual flow control setting for this channel. Possible values = OFF, RX, TX, RXTX, ON
lamode	<String>	Read-only	The mode(AUTO/MANNUAL) for the LA channel. Possible values = MANUAL, AUTO
autoneg	<Integer>	Read-only	Requested auto negotiation setting for this channel. Since no media are associated with LA, this setting has no effect.
autonegresult	<Integer>	Read-only	Actual auto negotiation setting for this channel.
tagged	<Integer>	Read-only	VLAN tags setting on this channel.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
taggedany	<Integer>	Read-only	Channel setting to accept/drop all tagged packets.
taggedautolearn	<Integer>	Read-only	Dynaminc vlan membership on this channel.
hangdetect	<Integer>	Read-only	Hang detect for this channel.
hangreset	<Integer>	Read-only	Hang reset for this channel.
linkstate	<Integer>	Read-only	The current state of the link associated with the interface. For logical interfaces (LA), the state of the link is dependent on the state of the slave interfaces. For the link to be UP at least one of the slave interfaces needs to be UP.
intfstate	<Integer>	Read-only	Current state of the specified interface. The interface state set to UP only if the link state is UP and administrative state is ENABLED.
rxpackets	<Integer>	Read-only	Number of bytes received by all the slave interfaces of the channel since the Citrix ADC was started or the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			interface statistics were cleared.
rxbytes	<Integer>	Read-only	Number of packets received by all member interfaces since the Citrix ADC was started or the interface statistics were cleared.
rxerrors	<Integer>	Read-only	Number of inbound packets dropped by the hardware of the slave interfaces since the Citrix ADC was started or the interface statistics were cleared. Possible causes of dropped packets are CRC, length (undersize or oversize), and alignment errors.
rxdrops	<Integer>	Read-only	Number of inbound packets dropped by the channel's slave interfaces. Commonly dropped packets are multicast frames, spanning tree BPDUs, packets destined to a MAC not owned by the Citrix ADC when L2 mode is disabled, or packets tagged for a VLAN that is not bound to the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			interface. In most healthy networks, this statistic increments at a steady rate regardless of traffic load. A sharp spike in dropped packets generally indicates an issue with connected L2 switches, such as a forwarding database overflow resulting in packets being broadcast on all ports.
txpackets	<Integer>	Read-only	Number of packets transmitted by slave interfaces of a channel since the Citrix ADC was started or the interface statistics were cleared.
txbytes	<Integer>	Read-only	Number of bytes transmitted by slave interfaces of a channel since the Citrix ADC was started or the interface statistics were cleared.
txerrors	<Integer>	Read-only	Number of outbound packets dropped by the hardware of a channel's slave interfaces since the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Citrix ADC was started or the interface statistics were cleared. Possible causes of dropped packets are length (undersize or oversize) errors and lack of resources.
txdrops	<Integer>	Read-only	Number of packets dropped in transmission by a channel's slave interfaces for one of the following reasons: (1) VLAN mismatch. (2) Oversized packets. (3) Interface congestion. (4) Loopback packets sent on non-loopback interface.
indisc	<Integer>	Read-only	Number of error-free inbound packets discarded by a channel's slave interfaces because of a lack of resources (for example, insufficient receive buffers).

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
outdisc	<Integer>	Read-only	Number of error-free outbound packets discarded by a channel's slave interfaces because of a lack of resources. This statistic is not available on: (1) 10G ports of Citrix ADC MPX 12500/12500/15500 -10G platforms. (2) 10G data ports on Citrix ADC MPX 17500/19500/21500 platforms.
fctls	<Integer>	Read-only	Number of times flow control is performed on a channel's slave interfaces because of pause frames.
hangs	<Integer>	Read-only	Number of hangs that occurred on the channel's slave interfaces.
stsstalls	<Integer>	Read-only	Number of status stalls that occurred on the channel's slave interfaces.
txstalls	<Integer>	Read-only	Number of Tx stalls happened that occurred on the channel's slave interfaces.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
rxstalls	<Integer>	Read-only	Number of Rx stalls that occurred on the channel's slave interfaces.
bdgmuted	<Integer>	Read-only	Number of times a channel's slave interfaces stopped transmitting and receiving packets because of MAC moves between ports.
vmac	<String>	Read-only	Virtual MAC of this channel.
vmac6	<String>	Read-only	Virtual MAC for IPv6 on this interface.
reqthroughput	<Integer>	Read-only	Minimum required throughput for an interface. Failover is triggered if the operating throughput of a Link Aggregation (LA) channel for which HAMON is ON falls below this value. Minimum value = 0 Maximum value = 500000
actthroughput	<Integer>	Read-only	Actual throughput for the interface.
backplane	<String>	Read-only	The cluster backplane status of the LA. If the status is enabled, the LA is

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			part of the cluster backplane. By default, the backplane status is disabled. Possible values = ENABLED, DISABLED
cleartime	<Integer>	Read-only	Time since the interface stats are cleared last time.
lacpmode	<String>	Read-only	The LACP mode of the specified interface. The possible values are: 1. Active: A port in active mode generates LACP protocol messages on a regular basis, regardless of any need expressed by its partner to receive them. 2. Passive: A port in passive mode generally does not transmit LACP messages unless its partner is in the active mode; that is, it does not speak unless spoken to.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			3. Disabled: Removes the interface from the LA channel. If this is only interface in the LA channel, the LA channel is also deleted. . Possible values = DISABLED, ACTIVE, PASSIVE
lacptimeout	<String>	Read-only	Time to wait for the LACPDU. If a LACPDU is not received within this interval, the Citrix ADC markes the link partner port as DOWN. Possible values: Long and Short. Long lacptimeout is 90 sec and Short LACP timeout is 3 sec. Possible values = LONG, SHORT
lacpactorpriority	<Integer>	Read-only	LACP Actor Priority. A LACP port priority is configured on each port using LACP. LACP uses the port priority with the port number to form the port identifier. The port

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			priority determines which ports should be put in standby mode when there is a hardware limitation that prevents all compatible ports from aggregating.
lacpactorportno	<Integer>	Read-only	LACP Actor port number. LACP uses the port priority with the port number to form the port identifier.
lacppartnerstate	<String>	Read-only	LACP Partner State. Whether the port is in Active or Passive negotiating state. Possible values = MANUAL, AUTO
lacppartnertimeout	<String>	Read-only	The timeout value for the information revieved in LACPDUs. It can have values as SHORT or LONG. The SHORT timeout is 3s and the LONG timeout is 90s. Possible values = LONG, SHORT
lacppartneraggregation	<String>	Read-only	The Aggregation flag indicates that the participant will allow the link to be used as part of an aggregate. Otherwise the link is

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			to be used as an individual link, i.e. not aggregated with any other. Possible values = NS_EMPTY_STR, AGG
lacppartnerinsync	<String>	Read-only	The Synchronization flag indicates that the transmitting participant.s mux component is in sync with the system id and key information transmitted. Possible values = NS_EMPTY_STR, SYNC
lacppartnercollecting	<String>	Read-only	The Collecting flag indicates that the participant.s collector, i.e. the reception component of the mux, is definitely on. If set the flag communicates collecting. Possible values = NS_EMPTY_STR, COLLECTING
lacppartnerdistributing	<String>	Read-only	The Distributing flag indicates that the participant.s distributor is not definitely off. If reset

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			the flag indicates not distributing. Possible values = NS_EMPTY_STR, DISTRIBUTING
lacppartnerdefaulted	<String>	Read-only	If the timer expires in the Expired state, the Receive Machine enters the Defaulted state. Possible values = NS_EMPTY_STR, DEFAULTED
lacppartnerexpired	<String>	Read-only	If the LACPDUs are received for timeout period, the Receive Machine enters the Expired state and the timer is restarted with the timeout value of SHORT timeout. Possible values = NS_EMPTY_STR, EXPIRED
lacppartnerpriority	<Integer>	Read-only	LACP Partner Priority. A LACP port priority is configured on each port using LACP. LACP uses the port priority with the port number to form the port identifier. The port priority determines which ports should be put

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			in standby mode when there is a hardware limitation that prevents all compatible ports from aggregating.
lacppartnersystemmac	<String>	Read-only	LACP Partner System MAC.
lacppartnersystempriority	<Integer>	Read-only	LACP Partner System Priority. The LACP partner's system priority. The values for the priority range from 0 to 65535. The lower the value, the higher the system priority. The switch with the lower system priority value determines which links between LACP partner are active and which are in the standby for each LACP Channel.
lacppartnerportno	<Integer>	Read-only	LACP Partner Port number. LACP uses the port priority with the port number to form the port identifier.
lacppartnerkey	<Integer>	Read-only	LACP Partner Key. The LACP key used by the partner port.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
lacpactoraggregation	<String>	Read-only	The Aggregation flag indicates that the participant will allow the link to be used as part of an aggregate. Otherwise the link is to be used as an individual link, i.e. not aggregated with any other. Possible values = NS_EMPTY_STR, AGG
lacpactorinsync	<String>	Read-only	The Synchronization flag indicates that the transmitting participant.s mux component is in sync with the system id and key information transmitted. Possible values = NS_EMPTY_STR, SYNC
lacpactorcollecting	<String>	Read-only	The Collecting flag indicates that the participant.s collector, i.e. the reception component of the mux, is definitely on. If set the flag communicates collecting. Possible values = NS_EMPTY_STR, COLLECTING

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
lacpactordistributing	<String>	Read-only	The Distributing flag indicates that the participant.s distributor is not definitely off. If reset the flag indicates not distributing. Possible values = NS_EMPTY_STR, DISTRIBUTING
lacpportmuxstate	<String>	Read-only	LACP Port MUX state. The state of the MUX control machine. The Mux Control Machine attaches the physical port to an aggregate port, using the Selection Logic to choose an appropriate port, and turns the distributor and collector for the physical port on or off as required by protocol information. Possible values = DETACHED, WAITING, ATTACHED, COLLECTING, DISTRIBUTING
lacpportrxstat	<String>	Read-only	LACP Port RX state. The state of the Receive machine. The Receive Machine maintains partner information,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			recording protocol information from LACPDUs sent by remote partner(s). Received information is subject to a timeout, and if sufficient time elapses the receive machine will revert to using default partner information. Possible values = INIT, PORT_DISABLED, LACP_DISABLED, EXPIRED, DEFAULTED, CURRENT
lacpportselectstate	<String>	Read-only	LACP Port SELECT state. The state of the SELECT state machine, It could be SELECTED or UNSELECTED. Possible values = UNSELECTED, SELECTED, STANDBY
lldpmode	<String>	Read-only	Link Layer Discovery Protocol (LLDP) mode for an interface. The resultant LLDP mode of an interface depends on the LLDP mode configured at the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			global and the interface levels. Possible values = NONE, TRANSMITTER, RECEIVER, TRANSCEIVER
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of

creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/channel **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"channel":{

<b>"id":<String_value>,

</b>"ifnum":<String[]_value>,

"state":<String_value>,

"mode":<String_value>,

"conndistr":<String_value>,

"macdistr":<String_value>,

"lamac":<String_value>,

"speed":<String_value>,
```

```
"flowctl":<String_value>,

"hamonitor":<String_value>,

"haheartbeat":<String_value>,

"tagall":<String_value>,

"trunk":<String_value>,

"ifalias":<String_value>,

"throughput":<Integer_value>,

"bandwidthhigh":<Integer_value>,

"bandwidthnormal":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/channel/ id_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/channel **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"channel":{

<b>"id":<String_value>,

</b>"state":<String_value>,

"mode":<String_value>,

"conndistr":<String_value>,

"macdistr":<String_value>,

"lamac":<String_value>,

"speed":<String_value>,

"mtu":<Integer_value>,

"flowctl":<String_value>,

"hamonitor":<String_value>,

"haheartbeat":<String_value>,

"tagall":<String_value>,

"trunk":<String_value>,

"ifalias":<String_value>,

"throughput":<Integer_value>,

"lrminthroughput":<Integer_value>,

"linkredundancy":<String_value>,

"bandwidthhigh":<Integer_value>,
```

```
"bandwidthnormal":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/channel? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"channel":{

<b>"id":<String_value>,

</b>"state":true,

"mode":true,

"conndistr":true,

"macdistr":true,

"speed":true,

"mtu":true,

"flowctl":true,

"hamonitor":true,

"haheartbeat":true,
```

```
"tagall":true,

"trunk":true,

"ifalias":true,

"throughput":true,

"lrminthroughput":true,

"linkredundancy":true,

"bandwidthhigh":true,

"bandwidthnormal":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/channel **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/channel? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/channel? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of channel resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/channel? **view=summary**

Use this query-parameter to get the summary output of channel resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/channel? **pagesize=#no;pageno=#no**

Use this query-parameter to get the channel resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "channel": [ {

"id":<String_value>,

"devicename":<String_value>,

"unit":<Integer_value>,

"description":<String_value>,

"flags":<Integer_value>,

"mtu":<Integer_value>,

"actualmtu":<Integer_value>,

"vlan":<Integer_value>,

"mac":<String_value>,

"lamac":<String_value>,
```

```
"uptime":<Integer_value>,

"downtime":<Integer_value>,

"reqmedia":<String_value>,

"reqspeed":<String_value>,

"reqduplex":<String_value>,

"reqflowcontrol":<String_value>,

"media":<String_value>,

"actspeed":<String_value>,

"duplex":<String_value>,

"actflowctl":<String_value>,

"mode":<String_value>,

"lamode":<String_value>,

"hamonitor":<String_value>,

"haheartbeat":<String_value>,

"state":<String_value>,

"autoneg":<Integer_value>,

"autonegresult":<Integer_value>,

"tagged":<Integer_value>,

"tagall":<String_value>,

"trunk":<String_value>,

"taggedany":<Integer_value>,

"taggedautolearn":<Integer_value>,
```

```
"hangdetect":<Integer_value>,

"hangreset":<Integer_value>,

"linkstate":<Integer_value>,

"intfstate":<Integer_value>,

"rxpackets":<Integer_value>,

"rxbytes":<Integer_value>,

"rxerrors":<Integer_value>,

"rxdrops":<Integer_value>,

"txpackets":<Integer_value>,

"txbytes":<Integer_value>,

"txerrors":<Integer_value>,

"txdrops":<Integer_value>,

"indisc":<Integer_value>,

"outdisc":<Integer_value>,

"fctls":<Integer_value>,

"hangs":<Integer_value>,

"stsstalls":<Integer_value>,

"txstalls":<Integer_value>,

"rxstalls":<Integer_value>,

"bdgmuted":<Integer_value>,

"vmac":<String_value>,

"vmac6":<String_value>,
```

```
"ifalias":<String_value>,

"reqthroughput":<Integer_value>,

"lrminthroughput":<Integer_value>,

"linkredundancy":<String_value>,

"actthroughput":<Integer_value>,

"bandwidthhigh":<Integer_value>,

"bandwidthnormal":<Integer_value>,

"ifnum":<String[]_value>,

"backplane":<String_value>,

"cleartime":<Integer_value>,

"lacpmode":<String_value>,

"lacptimeout":<String_value>,

"lacpactorpriority":<Integer_value>,

"lacpactorportno":<Integer_value>,

"lacppartnerstate":<String_value>,

"lacppartnertimeout":<String_value>,

"lacppartneraggregation":<String_value>,

"lacppartnerinsync":<String_value>,

"lacppartnercollecting":<String_value>,

"lacppartnerdistributing":<String_value>,

"lacppartnerdefaulted":<String_value>,

"lacppartnerexpired":<String_value>,
```

```
"lacppartnerpriority":<Integer_value>,

"lacppartnersystemmac":<String_value>,

"lacppartnersystempriority":<Integer_value>,

"lacppartnerportno":<Integer_value>,

"lacppartnerkey":<Integer_value>,

"lacpactoraggregation":<String_value>,

"lacpactorinsync":<String_value>,

"lacpactorcollecting":<String_value>,

"lacpactordistributing":<String_value>,

"lacpportmuxstate":<String_value>,

"lacpportrxstat":<String_value>,

"lacpportselectstate":<String_value>,

"lldpmode":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/channel/ id_value<String> **Query-parameters:**
attrs http:// <netscaler-ip-address> /nitro/v1/config/channel/ id_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/channel/ id_value<String> ? **view=summary**

Use this query-parameter to get the summary output of channel resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "channel": [ {

"id":<String_value>,

"devicename":<String_value>,

"unit":<Integer_value>,

"description":<String_value>,

"flags":<Integer_value>,

"mtu":<Integer_value>,

"actualmtu":<Integer_value>,

"vlan":<Integer_value>,

"mac":<String_value>,

"lamac":<String_value>,

"uptime":<Integer_value>,
```

```
"downtime":<Integer_value>,

"reqmedia":<String_value>,

"reqspeed":<String_value>,

"reqduplex":<String_value>,

"reqflowcontrol":<String_value>,

"media":<String_value>,

"actspeed":<String_value>,

"duplex":<String_value>,

"actflowctl":<String_value>,

"mode":<String_value>,

"lamode":<String_value>,

"hamonitor":<String_value>,

"haheartbeat":<String_value>,

"state":<String_value>,

"autoneg":<Integer_value>,

"autonegresult":<Integer_value>,

"tagged":<Integer_value>,

"tagall":<String_value>,

"trunk":<String_value>,

"taggedany":<Integer_value>,

"taggedautolearn":<Integer_value>,

"hangdetect":<Integer_value>,
```

```
"hangreset":<Integer_value>,

"linkstate":<Integer_value>,

"intfstate":<Integer_value>,

"rxpackets":<Integer_value>,

"rxbytes":<Integer_value>,

"rxerrors":<Integer_value>,

"rxdrops":<Integer_value>,

"txpackets":<Integer_value>,

"txbytes":<Integer_value>,

"txerrors":<Integer_value>,

"txdrops":<Integer_value>,

"indisc":<Integer_value>,

"outdisc":<Integer_value>,

"fctls":<Integer_value>,

"hangs":<Integer_value>,

"stsstalls":<Integer_value>,

"txstalls":<Integer_value>,

"rxstalls":<Integer_value>,

"bdgmuted":<Integer_value>,

"vmac":<String_value>,

"vmac6":<String_value>,

"ifalias":<String_value>,
```

```
"reqthroughput":<Integer_value>,

"lrminthroughput":<Integer_value>,

"linkredundancy":<String_value>,

"actthroughput":<Integer_value>,

"bandwidthhigh":<Integer_value>,

"bandwidthnormal":<Integer_value>,

"ifnum":<String[]_value>,

"backplane":<String_value>,

"cleartime":<Integer_value>,

"lacpmode":<String_value>,

"lacptimeout":<String_value>,

"lacpactorpriority":<Integer_value>,

"lacpactorportno":<Integer_value>,

"lacppartnerstate":<String_value>,

"lacppartnertimeout":<String_value>,

"lacppartneraggregation":<String_value>,

"lacppartnerinsync":<String_value>,

"lacppartnercollecting":<String_value>,

"lacppartnerdistributing":<String_value>,

"lacppartnerdefaulted":<String_value>,

"lacppartnerexpired":<String_value>,

"lacppartnerpriority":<Integer_value>,
```

```
"lacppartnersystemmac":<String_value>,

"lacppartnersystempriority":<Integer_value>,

"lacppartnerportno":<Integer_value>,

"lacppartnerkey":<Integer_value>,

"lacpactoraggregation":<String_value>,

"lacpactorinsync":<String_value>,

"lacpactorcollecting":<String_value>,

"lacpactordistributing":<String_value>,

"lacpportmuxstate":<String_value>,

"lacpportrxstat":<String_value>,

"lacpportselectstate":<String_value>,

"lldpmode":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/channel? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "channel": [ { "__count": "#no"} ] }
```

channel_binding

Binding object which returns the resources bound to channel.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
id	<String>	Read-write	ID of an LA channel or LA channel in cluster configuration whose details you want the Citrix ADC to display. Specify an LA channel in LA/x notation, where x can range from 1 to 8 or a cluster LA channel in CLA/x notation or Link redundant channel in LR/x notation , where x can range from 1 to 4. Minimum length = 1
channel_interface_binding	<channel_interface_binding[]>	Read-only	interface that can be bound to channel.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/channel_binding/ id_value<String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "channel_binding": [ {

"id":<String_value>,

"channel_interface_binding":<channel_interface_binding[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/channel_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/channel_binding?**bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "channel_binding": [ {

"id":<String_value>,

"channel_interface_binding":<channel_interface_binding[]_value>

}]}
```

channel_interface_binding

Binding object showing the interface that can be bound to channel.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
svmcmd	<Integer>	Read-write	New attribute added to identify the source of cmd, when SVM fires the nitro cmd, it will set the value of SVMCMD to be 1. . Default value: 0
id	<String>	Read-write	ID of the LA channel or the cluster LA channel to which you want to bind interfaces. Specify an LA channel in LA/x notation, where x can range from 1 to 8 or a cluster LA channel in CLA/x notation or Link redundant channel in LR/x notation , where

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			x can range from 1 to 4.
ifnum	<String[]>	Read-write	Interfaces to be bound to the LA channel of a Citrix ADC or to the LA channel of a cluster configuration. For an LA channel of a Citrix ADC, specify an interface in C/U notation (for example, 1/3). For an LA channel of a cluster configuration, specify an interface in N/C/U notation (for example, 2/1/3). where C can take one of the following values: * 0 - Indicates a management interface. * 1 - Indicates a 1 Gbps port. * 10 - Indicates a 10 Gbps port. U is a unique integer for representing an interface in a particular port group. N is the ID of the node to which an interface belongs in a cluster configuration. Use spaces to separate multiple entries.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
slavemedia	<Integer>	Read-only	Media type of the member interfaces.
slaveflowctl	<Integer>	Read-only	Flowcontrol of the member interfaces.
slavespeed	<Integer>	Read-only	Speed of the member interfaces.
lractiveintf	<Integer>	Read-only	LR set member interface state(active/inactive).
lamode	<String>	Read-only	The mode(AUTO/ MANNUAL) for the LA channel. Possible values = MANUAL, AUTO
slavetime	<Integer>	Read-only	UP time of the member interfaces.
slavestate	<Integer>	Read-only	State of the member interfaces.
slaveduplex	<Integer>	Read-only	Duplex of the member interfaces.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/channel_interface_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"channel_interface_binding":{

<b>"id":<String_value>,
```

```
</b><b>"ifnum":<String[]_value></b>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/channel_interface_binding/ id_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/channel_interface_binding/ id_value<String> ? **args= ifnum:<String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/channel_interface_binding/ id_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/channel_interface_binding/ id_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of channel_interface_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/channel_interface_binding/ id_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the channel_interface_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "channel_interface_binding": [ {

"svmcmd":<Integer_value>,

"id":<String_value>,

"ifnum":<String[]_value>,

"slavemedia":<Integer_value>,

"slaveflowctl":<Integer_value>,

"slavespeed":<Integer_value>,

"lractiveintf":<Integer_value>,

"lamode":<String_value>,

"slavetime":<Integer_value>,

"slavestate":<Integer_value>,

"slaveduplex":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/channel_interface_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/channel_interface_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "channel_interface_binding": [ {

"svmcmd":<Integer_value>,

"id":<String_value>,

"ifnum":<String[]_value>,

"slavemedia":<Integer_value>,

"slaveflowctl":<Integer_value>,

"slavespeed":<Integer_value>,

"lractiveintf":<Integer_value>,

"lamode":<String_value>,
```

```
"slavetime":<Integer_value>,

"slavestate":<Integer_value>,

"slaveduplex":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/channel_interface_binding/ id_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"channel_interface_binding": [ { "__count": "#no"} ] }
```

ci

Configuration for "CI" resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ifaces	<String>	Read-write	Interfaces that are critical for the appliance to operate in high availability mode.
_nextgenapiresource	<String>	Read-write	.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/ci

Query-parameters:

attrs

http:// <netscaler-ip-address> /nitro/v1/config/ci? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter

http:// <netscaler-ip-address> /nitro/v1/config/ci? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of ci resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view

http:// <netscaler-ip-address> /nitro/v1/config/ci? **view=summary**

Use this query-parameter to get the summary output of ci resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination

http:// <netscaler-ip-address> /nitro/v1/config/ci? **pagesize=#no;pageno=#no**

Use this query-parameter to get the ci resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "ci": [ {

"ifaces":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/ci? **count=yes**

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "ci": [ { "__count": "#no"} ] }
```

fis

Configuration for "FIS" resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the FIS to be created. Leading character must be a number or letter. Other characters allowed, after the first character, are @ _ - . (period) : (colon) # and space ( ). Note: In a cluster setup, the FIS name on each node must be unique. Minimum length = 1
ownernode	<Integer>	Read-write	ID of the cluster node for which you are creating the FIS. Can be configured only through the cluster IP address. Minimum value = 0 Maximum value = 31

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ifaces	<String>	Read-only	Interfaces to be bound to the FIS, in slot/port notation (for example, 1/3).
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/fis **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"fis":{

<b>"name":<String_value>,

</b>"ownernode":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/fis/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/fis **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/fis? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/fis? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of fis resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/fis? **view=summary**

Use this query-parameter to get the summary output of fis resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/fis? **pagesize=#no;pageno=#no**

Use this query-parameter to get the fis resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "fis": [ {

"name":<String_value>,

"ifaces":<String_value>,

"ownernode":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/fis/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/fis/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/fis/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of fis resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "fis": [ {

"name":<String_value>,

"ifaces":<String_value>,

"ownernode":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/fis? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "fis": [ { "__count": "#no"} ] }
```

fis_binding

Binding object which returns the resources bound to fis.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	The name of the FIS configured on the appliance. . Minimum length = 1
fis_channel_binding	<fis_channel_binding []>	Read-only	channel that can be bound to fis.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/fis_binding/ name_value<String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "fis_binding": [ {

"name":<String_value>,

"fis_channel_binding":<fis_channel_binding[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/fis_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/fis_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "fis_binding": [ {

"name":<String_value>,

"fis_channel_binding":<fis_channel_binding[]_value>

}]}
```

fis_channel_binding

Binding object showing the channel that can be bound to fis.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ifnum	<String>	Read-write	Interface to be bound to the FIS, specified in slot/port notation (for example, 1/3).
name	<String>	Read-write	The name of the FIS to which you want to bind interfaces. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ownernode	<Integer>	Read-write	ID of the cluster node for which you are creating the FIS. Can be configured only through the cluster IP address. Minimum value = 0 Maximum value = 31
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/fis_channel_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"fis_channel_binding":{

<b>"name":<String_value>,

</b><b>"ifnum":<String_value></b>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/fis_channel_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/fis_channel_binding/ name_value<String> ? **args= ifnum:<String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/fis_channel_binding/ name_value<String>
Query-parameters: filter http:// <netscaler-ip-address> /nitro/v1/config/fis_channel_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of fis_channel_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/fis_channel_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the fis_channel_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "fis_channel_binding": [ {

"ifnum":<String_value>,

"name":<String_value>,

"ownernode":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/fis_channel_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/fis_channel_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "fis_channel_binding": [ {

"ifnum":<String_value>,

"name":<String_value>,
```

```
"ownernode":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/fis_channel_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"fis_channel_binding": [ { "__count": "#no"} ] }
```

fis_interface_binding

Binding object showing the interface that can be bound to fis.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ifnum	<String>	Read-write	Interface to be bound to the FIS, specified in slot/port notation (for example, 1/3).

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	The name of the FIS to which you want to bind interfaces. Minimum length = 1
ownernode	<Integer>	Read-write	ID of the cluster node for which you are creating the FIS. Can be configured only through the cluster IP address. Minimum value = 0 Maximum value = 31

Operations

(click to see Properties)

- ADD
- DELETE

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/fis_interface_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"fis_interface_binding":{

<b>"name":<String_value>,

</b><b>"ifnum":<String_value></b>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/fis_interface_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/fis_interface_binding/ name_value<String> ? **args= ifnum:<String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

forwardingsession

Configuration for session forward resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the forwarding session rule. Can begin with a letter, number, or the underscore character (_), and can consist of letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after the rule is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			single quotation marks (for example, "my rule" or 'my rule'). Minimum length = 1
network	<String>	Read-write	An IPv4 network address or IPv6 prefix of a network from which the forwarded traffic originates or to which it is destined. Minimum length = 1
netmask	<String>	Read-write	Subnet mask associated with the network. Minimum length = 1
acl6name	<String>	Read-write	Name of any configured ACL6 whose action is ALLOW. The rule of the ACL6 is used as a forwarding session rule. Minimum length = 1
aclname	<String>	Read-write	Name of any configured ACL whose action is ALLOW. The rule of the ACL is used as a forwarding session rule. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
td	<Integer>	Read-write	Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0. Minimum value = 0 Maximum value = 4094
connfailover	<String>	Read-write	Synchronize connection information with the secondary appliance in a high availability (HA) pair. That is, synchronize all connection-related information for the forwarding session. Default value: DISABLED Possible values = ENABLED, DISABLED
sourceroutecache	<String>	Read-write	Cache the source ip address and mac address of the DA servers. Default value: DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ENABLED, DISABLED
processlocal	<String>	Read-write	Enabling this option on forwarding session will not steer the packet to flow processor. Instead, packet will be routed. Default value: DISABLED Possible values = ENABLED, DISABLED
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- UPDATE
- DELETE
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/forwardingsession **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"forwardingsession":{

<b>"name":<String_value>,

</b>"network":<String_value>,

"netmask":<String_value>,

"acl6name":<String_value>,

"aclname":<String_value>,

"td":<Integer_value>,
```

```
"connfailover":<String_value>,

"sourceroutecache":<String_value>,

"processlocal":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/forwardingsession **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"forwardingsession":{

<b>"name":<String_value>,

</b>"connfailover":<String_value>,

"sourceroutecache":<String_value>,

"processlocal":<String_value>,

"acl6name":<String_value>,

"aclname":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/forwardingsession/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/forwardingsession **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/forwardingsession? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/forwardingsession? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of forwardingsession resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/forwardingsession? **view=summary**

Use this query-parameter to get the summary output of forwardingsession resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/forwardingsession? **pagesize=#no;pageno=#no**

Use this query-parameter to get the forwardingsession resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "forwardingsession": [ {

"name":<String_value>,

"network":<String_value>,

"netmask":<String_value>,

"td":<Integer_value>,

"aclname":<String_value>,

"acl6name":<String_value>,

"connfailover":<String_value>,

"sourceroutecache":<String_value>,

"processlocal":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/forwardingsession/ name_value<String>
Query-parameters: attrs http:// <netscaler-ip-address> /nitro/v1/config/forwardingsession/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/forwardingsession/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of forwardingsession resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "forwardingsession": [ {

"name":<String_value>,

"network":<String_value>,

"netmask":<String_value>,

"td":<Integer_value>,
```

```
"aclname":<String_value>,

"acl6name":<String_value>,

"connfailover":<String_value>,

"sourceroutecache":<String_value>,

"processlocal":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/forwardingsession? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "forwardingsession": [ { "__count": "#no"} ] }
```

inat

Configuration for inbound nat resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the Inbound NAT (INAT) entry. Leading character must be a number or letter. Other characters allowed, after the first character, are @ _ - . (period) : (colon) # and space ( ). Minimum length = 1
publicip	<String>	Read-write	Public IP address of packets received on the Citrix ADC. Can be aNetScaler-owned VIP or VIP6 address. Minimum length = 1
privateip	<String>	Read-write	IP address of the server to which the packet is sent by the Citrix ADC. Can be an IPv4 or IPv6 address. Minimum length = 1
mode	<String>	Read-write	Stateless translation. Possible values = STATELESS
tcpproxy	<String>	Read-write	Enable TCP proxy, which enables the Citrix ADC to optimize the RNAT

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			TCP traffic by using Layer 4 features. Default value: DISABLED Possible values = ENABLED, DISABLED
ftp	<String>	Read-write	Enable the FTP protocol on the server for transferring files between the client and the server. Default value: DISABLED Possible values = ENABLED, DISABLED
tftp	<String>	Read-write	To enable/disable TFTP (Default DISABLED). Default value: DISABLED Possible values = ENABLED, DISABLED
usip	<String>	Read-write	Enable the Citrix ADC to retain the source IP address of packets before sending the packets to the server.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ON, OFF
usnip	<String>	Read-write	Enable the Citrix ADC to use a SNIP address as the source IP address of packets before sending the packets to the server. Possible values = ON, OFF
proxyip	<String>	Read-write	Unique IP address used as the source IP address in packets sent to the server. Must be a MIP or SNIP address.
useproxyport	<String>	Read-write	Enable the Citrix ADC to proxy the source port of packets before sending the packets to the server. Default value: ENABLED Possible values = ENABLED, DISABLED
td	<Integer>	Read-write	Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			an ID, the entity becomes part of the default traffic domain, which has an ID of 0. Minimum value = 0 Maximum value = 4094
connfailover	<String>	Read-write	Synchronize connection information with the secondary appliance in a high availability (HA) pair. That is, synchronize all connection-related information for the INAT session. Default value: DISABLED Possible values = ENABLED, DISABLED
flags	<Integer>	Read-only	Flags for different modes.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE

- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/inat **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"inat":{

<b>"name":<String_value>,

</b><b>"publicip":<String_value>,

</b><b>"privateip":<String_value>,

</b>"mode":<String_value>,

"tcpproxy":<String_value>,

"ftp":<String_value>,

"tftp":<String_value>,

"usip":<String_value>,

"usnip":<String_value>,

"proxyip":<String_value>,

"useproxyport":<String_value>,

"td":<Integer_value>,

"connfailover":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/inat/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/inat **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"inat":{

<b>"name":<String_value>,

</b>"privateip":<String_value>,

"tcpproxy":<String_value>,

"ftp":<String_value>,

"tftp":<String_value>,

"usip":<String_value>,

"usnip":<String_value>,

"proxyip":<String_value>,

"useproxyport":<String_value>,

"connfailover":<String_value>,

"mode":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/inat? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"inat":{

<b>"name":<String_value>,

</b>"tcpproxy":true,

"ftp":true,

"tftp":true,

"usip":true,

"usnip":true,

"proxyip":true,

"useproxyport":true,

"connfailover":true,

"mode":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/inat **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/inat? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/inat? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of inat resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/inat? **view=summary**

Use this query-parameter to get the summary output of inat resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/inat? **pagesize=#no;pageno=#no**

Use this query-parameter to get the inat resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "inat": [ {

"name":<String_value>,

"publicip":<String_value>,

"privateip":<String_value>,

"proxyip":<String_value>,

"tcpproxy":<String_value>,

"ftp":<String_value>,

"tftp":<String_value>,

"usip":<String_value>,

"usnip":<String_value>,

"useproxyport":<String_value>,

"flags":<Integer_value>,

"mode":<String_value>,

"connfailover":<String_value>,

"td":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/inat/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/inat/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/inat/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of inat resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "inat": [ {

"name":<String_value>,

"publicip":<String_value>,

"privateip":<String_value>,

"proxyip":<String_value>,

"tcpproxy":<String_value>,

"ftp":<String_value>,

"tftp":<String_value>,

"usip":<String_value>,

"usnip":<String_value>,
```

```
"useproxyport":<String_value>,

"flags":<Integer_value>,

"mode":<String_value>,

"connfailover":<String_value>,

"td":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/inat? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "inat": [ { "__count": "#no"} ] }
```

inatparam

Configuration for INAT parameter resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
nat46v6prefix	<String>	Read-write	The prefix used for translating packets received from private IPv6 servers into IPv4 packets. This prefix has a length of 96 bits (128-32 = 96). The IPv6 servers embed the destination IP address of the IPv4 servers or hosts in the last 32 bits of the destination IP address field of the IPv6 packets. The first 96 bits of the destination IP address field are set as the IPv6 NAT prefix. IPv6 packets addressed to this prefix have to be routed to the Citrix ADC to ensure that the IPv6-IPv4 translation is done by the appliance.
td	<Integer>	Read-write	Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			domain, which has an ID of 0. Default value: 0 Minimum value = 0 Maximum value = 4094
nat46ignoretos	<String>	Read-write	Ignore TOS. Default value: NO Possible values = YES, NO
nat46zerochecksum	<String>	Read-write	Calculate checksum for UDP packets with zero checksum. Default value: ENABLED Possible values = ENABLED, DISABLED
nat46v6mtu	<Integer>	Read-write	MTU setting for the IPv6 side. If the incoming IPv4 packet greater than this, either fragment or send icmp need fragmentation error. Default value: 1280 Minimum value = 1280 Maximum value = 9216

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
nat46fragheader	<String>	Read-write	When disabled, translator will not insert IPv6 fragmentation header for non fragmented IPv4 packets. Default value: ENABLED Possible values = ENABLED, DISABLED
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/inatparam **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"inatparam":{

"nat46v6prefix":<String_value>,

"td":<Integer_value>,

"nat46ignoretos":<String_value>,

"nat46zerochecksum":<String_value>,

"nat46v6mtu":<Integer_value>,

"nat46fragheader":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/inatparam? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"inatparam":{

"nat46v6prefix":true,

"td":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/inatparam **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/inatparam? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/inatparam? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of inatparam resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/inatparam? **view=summary**

Use this query-parameter to get the summary output of inatparam resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/inatparam? **pagesize=#no;pageno=#no**

Use this query-parameter to get the inatparam resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "inatparam": [ {

"td":<Integer_value>,

"nat46v6prefix":<String_value>,

"nat46ignoretos":<String_value>,

"nat46zerochecksum":<String_value>,

"nat46v6mtu":<Integer_value>,
```

```
"nat46fragheader":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/inatparam/ td_value<Integer> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/inatparam/ td_value<Integer> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/inatparam/ td_value<Integer> ? **view=summary**

Use this query-parameter to get the summary output of inatparam resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "inatparam": [ {

"td":<Integer_value>,

"nat46v6prefix":<String_value>,

"nat46ignoretos":<String_value>,

"nat46zerochecksum":<String_value>,

"nat46v6mtu":<Integer_value>,

"nat46fragheader":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/inatparam? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "inatparam": [ { "__count": "#no"} ] }
```

interfacepair

Configuration for "Interface Pair" resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
id	<Integer>	Read-write	The Interface pair id. Minimum value = 1 Maximum value = 255
ifnum	<String[]>	Read-write	The constituent interfaces in the interface pair. Minimum length = 1
ifaces	<String>	Read-only	Names of all member interfaces of this Interface Pair.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/interfacepair **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"interfacepair":{

<b>"id":<Integer_value>,

</b><b>"ifnum":<String[]_value>

</b>}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/interfacepair/ id_value<Integer> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/interfacepair **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/interfacepair? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/interfacepair? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of interfacepair resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/interfacepair? **view=summary**

Use this query-parameter to get the summary output of interfacepair resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/interfacepair? **pagesize=#no;pageno=#no**

Use this query-parameter to get the interfacepair resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "interfacepair": [ {

"id":<Integer_value>,

"ifnum":<String[]_value>,

"ifaces":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/interfacepair/ id_value<Integer> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/interfacepair/ id_value<Integer> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/interfacepair/ id_value<Integer> ? **view=summary**

Use this query-parameter to get the summary output of interfacepair resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "interfacepair": [ {

"id":<Integer_value>,

"ifnum":<String[]_value>,

"ifaces":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/interfacepair? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "interfacepair": [ { "__count": "#no"} ] }
```

ip6tunnel

Configuration for ip6 Tunnel resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the IPv6 Tunnel. Cannot be changed after the service group is created. Must begin with a number or letter, and can consist of letters, numbers, and the @ _ - . (period) : (colon) # and space ( ) characters. Minimum length = 1 Maximum length = 31

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
remote	<String>	Read-write	An IPv6 address of the remote Citrix ADC used to set up the tunnel. Minimum length = 1
local	<String>	Read-write	An IPv6 address of the local Citrix ADC used to set up the tunnel.
ownergroup	<String>	Read-write	The owner node group in a Cluster for the tunnel. Default value: DEFAULT_NG Minimum length = 1
remoteip	<String>	Read-only	The remote IP address or subnet of the tunnel.
type	<Integer>	Read-only	The type of this tunnel.
encapip	<String>	Read-only	The effective local IP address of the tunnel. Used as the source of the encapsulated packets.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD

- DELETE
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/ip6tunnel **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"ip6tunnel":{

<b>"name":<String_value>,

</b><b>"remote":<String_value>,

</b><b>"local":<String_value>,

</b>"ownergroup":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/ip6tunnel/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/ip6tunnel **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ip6tunnel? **args=name: <String_value> ,remote: <String_value>**

Use this query-parameter to get ip6tunnel resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/config/ip6tunnel? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/ip6tunnel? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of ip6tunnel resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/ip6tunnel? **view=summary**

Use this query-parameter to get the summary output of ip6tunnel resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/ip6tunnel? **pagesize=#no;pageno=#no**

Use this query-parameter to get the ip6tunnel resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "ip6tunnel": [ {

name:<String_value>,remote:<String_value>"remoteip":<String_value>,

"local":<String_value>,

"type":<Integer_value>,

"encapip":<String_value>,
```

```
"ownergroup":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/ip6tunnel/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/ip6tunnel/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/ip6tunnel/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of ip6tunnel resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "ip6tunnel": [ {

name:<String_value>,remote:<String_value>"remoteip":<String_value>,

"local":<String_value>,

"type":<Integer_value>,

"encapip":<String_value>,

"ownergroup":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/ip6tunnel? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "ip6tunnel": [ { "__count": "#no"} ] }
```

ip6tunnelparam

Configuration for ip6 tunnel parameter resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
srcip	<String>	Read-write	Common source IPv6 address for all IPv6 tunnels. Must be a SNIP6 or VIP6 address. Minimum length = 1
dropfrag	<String>	Read-write	Drop any packet that requires fragmentation. Default value: NO Possible values = YES, NO
dropfragcputhreshold	<Integer>	Read-write	Threshold value, as a percentage of CPU usage, at which to drop packets that require fragmentation. Applies only if dropFragparameter is set to NO. Minimum value = 1 Maximum value = 100
srciproundrobin	<String>	Read-write	Use a different source IPv6 address for each new session through a particular IPv6 tunnel, as determined by round robin selection of one of the SNIP6

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			addresses. This setting is ignored if a common global source IPv6 address has been specified for all the IPv6 tunnels. This setting does not apply to a tunnel for which a source IPv6 address has been specified. Default value: NO Possible values = YES, NO
useclientsourceipv6	<String>	Read-write	Use client source IPv6 address as source IPv6 address for outer tunnel IPv6 header. Default value: NO Possible values = YES, NO
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- UPDATE
- UNSET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/ip6tunnelparam **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"ip6tunnelparam":{

"srcip":<String_value>,

"dropfrag":<String_value>,

"dropfragcputhreshold":<Integer_value>,

"srciproundrobin":<String_value>,

"useclientsourceipv6":<String_value>
```

```
}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/ip6tunnelparam? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"ip6tunnelparam":{

"srcip":true,

"dropfrag":true,

"dropfragcputhreshold":true,

"srciproundrobin":true,

"useclientsourceipv6":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/ip6tunnelparam **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "ip6tunnelparam": [ {

"srcip":<String_value>,

"dropfrag":<String_value>,

"dropfragcputhreshold":<Integer_value>,

"srciproundrobin":<String_value>,

"useclientsourceipv6":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

ipset

Configuration for network ipset resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the IP set. Must begin with a letter, number, or the underscore character (_), and can consist of letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore characters. Cannot be changed after the IP set is created. Choose a name that helps identify the IP set. Minimum length = 1
td	<Integer>	Read-write	Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0. Minimum value = 0 Maximum value = 4094
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/ipset **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"ipset":{

<b>"name":<String_value>,

</b>"td":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/ipset/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/ipset **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/ipset? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/ipset? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of ipset resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/ipset? **view=summary**

Use this query-parameter to get the summary output of ipset resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/ipset? **pagesize=#no;pageno=#no**

Use this query-parameter to get the ipset resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "ipset": [ {

"name":<String_value>,

"td":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/ipset/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/ipset/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/ipset/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of ipset resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "ipset": [ {

"name":<String_value>,

"td":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/ipset? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "ipset": [ { "__count": "#no"} ] }
```

ipset_binding

Binding object which returns the resources bound to ipset.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the IP set whose details you want to display. Minimum length = 1
ipset_nsip6_binding	<ipset_nsip6_binding []>	Read-only	nsip6 that can be bound to ipset.
ipset_nsip_binding	<ipset_nsip_binding[] >	Read-only	nsip that can be bound to ipset.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/ipset_binding/ name_value<String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "ipset_binding": [ {

"name":<String_value>,

"ipset_nsip6_binding":<ipset_nsip6_binding[]_value>,

"ipset_nsip_binding":<ipset_nsip_binding[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/ipset_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ipset_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "ipset_binding": [ {

"name":<String_value>,

"ipset_nsip6_binding":<ipset_nsip6_binding[]_value>,

"ipset_nsip_binding":<ipset_nsip_binding[]_value>

}]}
```

ipset_nsip6_binding

Binding object showing the nsip6 that can be bound to ipset.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the IP set to which to bind IP addresses. Minimum length = 1
ipaddress	<String>	Read-write	One or more IP addresses bound to the IP set. Minimum length = 1
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/ipset_nsip6_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"ipset_nsip6_binding":{

<b>"name":<String_value>,

</b><b>"ipaddress":<String_value></b>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/ipset_nsip6_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ipset_nsip6_binding/ name_value<String> ? **args= ipaddress:<String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/ipset_nsip6_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ipset_nsip6_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of ipset_nsip6_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ipset_nsip6_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the ipset_nsip6_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "ipset_nsip6_binding": [ {

"name":<String_value>,

"ipaddress":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/ipset_nsip6_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ ipset_nsip6_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "ipset_nsip6_binding": [ {

"name":<String_value>,

"ipaddress":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/ipset_nsip6_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"ipset_nsip6_binding": [ { "__count": "#no"} ] }
```

ipset_nsip_binding

Binding object showing the nsip that can be bound to ipset.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ipaddress	<String>	Read-write	One or more IP addresses bound to the IP set. Minimum length = 1
name	<String>	Read-write	Name of the IP set to which to bind IP addresses. Minimum length = 1
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/ipset_nsip_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"ipset_nsip_binding":{

<b>"name":<String_value>,

</b><b>"ipaddress":<String_value></b>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/ipset_nsip_binding/ name_value<String>
Query-parameters: args http:// <netscaler-ip-address> /nitro/v1/config/ipset_nsip_binding/ name_value<String> ? **args= ipaddress:<String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/ipset_nsip_binding/ name_value<String>
Query-parameters: filter http:// <netscaler-ip-address> /nitro/v1/config/ipset_nsip_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of ipset_nsip_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ipset_nsip_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the ipset_nsip_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "ipset_nsip_binding": [ {

"ipaddress":<String_value>,

"name":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/ipset_nsip_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ipset_nsip_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "ipset_nsip_binding": [ {

"ipaddress":<String_value>,

"name":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/ipset_nsip_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"ipset_nsip_binding": [ { "__count": "#no"} ] }
```

iptunnel

Configuration for ip Tunnel resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the IP tunnel. Leading character must be a number or letter. Other characters allowed, after the first character, are @ _ - . (period) : (colon) # and space ( ). Minimum length = 1
remote	<String>	Read-write	Public IPv4 address, of the remote device, used to set up the tunnel. For this parameter, you can alternatively specify a network address. Minimum length = 1
remotesubnetmask	<String>	Read-write	Subnet mask of the remote IP address of the tunnel.
local	<String>	Read-write	Type of Citrix ADC owned public IPv4 address, configured on the local Citrix ADC and used to set up the tunnel.
protocol	<String>	Read-write	Name of the protocol to be used on this tunnel. Default value: IPIP Possible values = IPIP, GRE, IPSEC, UDP, GENEVE

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
vnid	<Integer>	Read-write	Virtual network identifier (VNID) is the value that identifies a specific virtual network in the data plane. Minimum value = 1 Maximum value = 16777215
vlantagging	<String>	Read-write	Option to select Vlan Tagging. Default value: DISABLED Possible values = ENABLED, DISABLED
destport	<Integer>	Read-write	Specifies UDP destination port for Geneve packets. Default port is 6081. Default value: 6081 Minimum value = 1024 Maximum value = 65535
tosinherit	<String>	Read-write	Default behavior is to copy the ToS field of the internal IP Packet (Payload) to the outer IP packet (Transport packet). But the user can configure a new ToS

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			field using this option. Default value: ENABLED Possible values = ENABLED, DISABLED
grepayload	<String>	Read-write	The payload GRE will carry. Default value: ETHERNETwithDOT1Q Possible values = ETHERNETwithDOT1Q, ETHERNET, IP
ipsecprofilename	<String>	Read-write	Name of IPSec profile to be associated. Default value: "ns_ipsec_default_profile"
vlan	<Integer>	Read-write	The vlan for mulicast packets. Minimum value = 1 Maximum value = 4094
ownergroup	<String>	Read-write	The owner node group in a Cluster for the iptunnel.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: DEFAULT_NG Minimum length = 1
sysname	<String>	Read-only	The name of the ip tunnel.
type	<Integer>	Read-only	The type of this tunnel.
encapip	<String>	Read-only	The effective local IP address of the tunnel. Used as the source of the encapsulated packets.
channel	<Integer>	Read-only	The tunnel that is bound to a netbridge.
tunneltype	<String[]>	Read-only	Indicates that a tunnel is User-Configured, Internal or DELETE-IN-PROGRESS. Possible values = Configured, Delete-In-Progress
ipsectunnelstatus	<String>	Read-only	Whether the ipsec on this tunnel is up or down. Possible values = DOWN, UP, PARTIAL-UP, UNKNOWN

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
refcnt	<Integer>	Read-only	Number of PBRs to bound to this iptunnel.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET (ALL)
- GET
- COUNT
- UPDATE
- UNSET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/iptunnel **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"iptunnel":{

<b>"name":<String_value>,

</b><b>"remote":<String_value>,

</b><b>"remotesubnetmask":<String_value>,

</b><b>"local":<String_value>,

</b>"protocol":<String_value>,

"vnid":<Integer_value>,

"vlantagging":<String_value>,

"destport":<Integer_value>,

"tosinherit":<String_value>,

"grepayload":<String_value>,

"ipsecprofilename":<String_value>,
```

```
"vlan":<Integer_value>,

"ownergroup":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/iptunnel/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/iptunnel **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"iptunnel":{

<b>"name":<String_value>,

</b>"vlantagging":<String_value>,

"destport":<Integer_value>,
```

```
"tosinherit":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/iptunnel? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"iptunnel":{

<b>"name":<String_value>,

</b>"vlantagging":true,

"destport":true,

"tosinherit":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/iptunnel **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/iptunnel? **args=remote: <String_value> ,remotesubnetmask: <String_value> ,name: <String_value>**

Use this query-parameter to get iptunnel resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/config/iptunnel? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/iptunnel? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of iptunnel resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/iptunnel? **view=summary**

Use this query-parameter to get the summary output of iptunnel resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/iptunnel? **pagesize=#no;pageno=#no**

Use this query-parameter to get the iptunnel resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "iptunnel": [ {

remote:<String_value>,remotesubnetmask:<String_value>,name:<String_value>"
sysname":<String_value>,

"local":<String_value>,

"protocol":<String_value>,

"grepayload":<String_value>,

"type":<Integer_value>,

"encapip":<String_value>,

"channel":<Integer_value>,

"ipsecprofilename":<String_value>,

"vlan":<Integer_value>,

"tunneltype":<String[]_value>,

"ipsectunnelstatus":<String_value>,

"ownergroup":<String_value>,

"refcnt":<Integer_value>,

"vnid":<Integer_value>,

"vlantagging":<String_value>,

"destport":<Integer_value>,

"tosinherit":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/iptunnel/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/iptunnel/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/iptunnel/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of iptunnel resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "iptunnel": [ {

remote:<String_value>,remotesubnetmask:<String_value>,name:<String_value>"
sysname":<String_value>,

"local":<String_value>,

"protocol":<String_value>,
```

```
"grepayload":<String_value>,

"type":<Integer_value>,

"encapip":<String_value>,

"channel":<Integer_value>,

"ipsecprofilename":<String_value>,

"vlan":<Integer_value>,

"tunneltype":<String[]_value>,

"ipsectunnelstatus":<String_value>,

"ownergroup":<String_value>,

"refcnt":<Integer_value>,

"vnid":<Integer_value>,

"vlantagging":<String_value>,

"destport":<Integer_value>,

"tosinherit":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/iptunnel? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "iptunnel": [ { "__count": "#no"} ] }
```

iptunnelparam

Configuration for ip tunnel parameter resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
srcip	<String>	Read-write	Common source-IP address for all tunnels. For a specific tunnel, this global setting is overridden if you have specified another source IP address. Must be a MIP or SNIP address. Minimum length = 1
dropfrag	<String>	Read-write	Drop any IP packet that requires fragmentation before it is sent through the tunnel. Default value: NO

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = YES, NO
dropfragcputhreshold	<Integer>	Read-write	Threshold value, as a percentage of CPU usage, at which to drop packets that require fragmentation to use the IP tunnel. Applies only if dropFragparameter is set to NO. The default value, 0, specifies that this parameter is not set. Minimum value = 1 Maximum value = 100
srciproundrobin	<String>	Read-write	Use a different source IP address for each new session through a particular IP tunnel, as determined by round robin selection of one of the SNIP addresses. This setting is ignored if a common global source IP address has been specified for all the IP tunnels. This setting does not apply to a tunnel for which a source IP address has been specified.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: NO Possible values = YES, NO
enablestrictrx	<String>	Read-write	Strict PBR check for IPSec packets received through tunnel. Default value: NO Possible values = YES, NO
enablestricttx	<String>	Read-write	Strict PBR check for packets to be sent IPSec protected. Default value: NO Possible values = YES, NO
mac	<String>	Read-write	The shared MAC used for shared IP between cluster nodes/HA peers.
useclientsourceip	<String>	Read-write	Use client source IP as source IP for outer tunnel IP header. Default value: NO Possible values = YES, NO
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- UPDATE
- UNSET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/iptunnelparam **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"iptunnelparam":{

"srcip":<String_value>,

"dropfrag":<String_value>,

"dropfragcputhreshold":<Integer_value>,

"srciproundrobin":<String_value>,

"enablestrictrx":<String_value>,

"enablestricttx":<String_value>,

"mac":<String_value>,

"useclientsourceip":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/iptunnelparam? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"iptunnelparam":{

"srcip":true,

"dropfrag":true,
```

```
"dropfragcputhreshold":true,

"srciproundrobin":true,

"enablestrictrx":true,

"enablestricttx":true,

"mac":true,

"useclientsourceip":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/iptunnelparam **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "iptunnelparam": [ {

"srcip":<String_value>,
```

```
"dropfrag":<String_value>,

"dropfragcputhreshold":<Integer_value>,

"srciproundrobin":<String_value>,

"enablestrictrx":<String_value>,

"enablestricttx":<String_value>,

"mac":<String_value>,

"useclientsourceip":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

ipv6

Configuration for ip v6 resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ralearning	<String>	Read-write	Enable the Citrix ADC to learn about various routes from Router Advertisement (RA) and Router Solicitation (RS) messages sent by the routers. Default value: DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ENABLED, DISABLED
routerredirection	<String>	Read-write	Enable the Citrix ADC to do Router Redirection. Default value: DISABLED Possible values = ENABLED, DISABLED
ndbasereachtime	<Integer>	Read-write	Base reachable time of the Neighbor Discovery (ND6) protocol. The time, in milliseconds, that the Citrix ADC assumes an adjacent device is reachable after receiving a reachability confirmation. Default value: 30000 Minimum value = 1
ndretransmissiontime	<Integer>	Read-write	Retransmission time of the Neighbor Discovery (ND6) protocol. The time, in milliseconds, between retransmitted Neighbor Solicitation (NS) messages, to an adjacent device.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: 1000 Minimum value = 1
natprefix	<String>	Read-write	Prefix used for translating packets from private IPv6 servers to IPv4 packets. This prefix has a length of 96 bits (128-32 = 96). The IPv6 servers embed the destination IP address of the IPv4 servers or hosts in the last 32 bits of the destination IP address field of the IPv6 packets. The first 96 bits of the destination IP address field are set as the IPv6 NAT prefix. IPv6 packets addressed to this prefix have to be routed to the Citrix ADC to ensure that the IPv6-IPv4 translation is done by the appliance.
td	<Integer>	Read-write	Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			default traffic domain, which has an ID of 0. Default value: 0 Minimum value = 0 Maximum value = 4094
dodad	<String>	Read-write	Enable the Citrix ADC to do Duplicate Address Detection (DAD) for all the Citrix ADC owned IPv6 addresses regardless of whether they are obtained through stateless auto configuration, DHCPv6, or manual configuration. Default value: DISABLED Possible values = ENABLED, DISABLED
usipnatprefix	<String>	Read-write	IPV6 NATPREFIX used in NAT46 scenario when USIP is turned on.
basereachtime	<Integer>	Read-only	ND6 base reachable time (ms).

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
reachtime	<Integer>	Read-only	ND6 computed reachable time (ms).
ndreachtime	<Integer>	Read-only	ND6 computed reachable time (ms).
retransmissiontime	<Integer>	Read-only	ND6 retransmission time (ms).
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.
- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/ipv6 **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"ipv6":{

"ralearning":<String_value>,

"routerredirection":<String_value>,

"ndbasereachtime":<Integer_value>,

"ndretransmissiontime":<Integer_value>,

"natprefix":<String_value>,

"td":<Integer_value>,

"dodad":<String_value>,

"usipnatprefix":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/ipv6? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"ipv6":{

"ralearning":true,

"routerredirection":true,

"ndbasereachtime":true,

"ndretransmissiontime":true,

"natprefix":true,

"td":<Integer_value>,

"dodad":true,

"usipnatprefix":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/ipv6 **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/ipv6? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/ipv6? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of ipv6 resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/ipv6? **view=summary**

Use this query-parameter to get the summary output of ipv6 resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/ipv6? **pagesize=#no;pageno=#no**

Use this query-parameter to get the ipv6 resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "ipv6": [ {

"td":<Integer_value>,
```

```
"ralearning":<String_value>,

"routerredirection":<String_value>,

"basereachtime":<Integer_value>,

"ndbasereachtime":<Integer_value>,

"reachtime":<Integer_value>,

"ndreachtime":<Integer_value>,

"retransmissiontime":<Integer_value>,

"ndretransmissiontime":<Integer_value>,

"natprefix":<String_value>,

"dodad":<String_value>,

"usipnatprefix":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/ipv6/ td_value<Integer> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/ipv6/ td_value<Integer> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/ipv6/ td_value<Integer> ? **view=summary**

Use this query-parameter to get the summary output of ipv6 resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "ipv6": [ {

"td":<Integer_value>,

"ralearning":<String_value>,

"routerredirection":<String_value>,

"basereachtime":<Integer_value>,

"ndbasereachtime":<Integer_value>,

"reachtime":<Integer_value>,

"ndreachtime":<Integer_value>,

"retransmissiontime":<Integer_value>,

"ndretransmissiontime":<Integer_value>,

"natprefix":<String_value>,

"dodad":<String_value>,

"usipnatprefix":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

```
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/ipv6? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "ipv6": [ { "__count": "#no"} ] }
```

l2param

Configuration for Layer 2 related parameter resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
mbfpeermacupdate	<Integer>	Read-write	When mbf_instant_learning is enabled, learn any changes in peer's MAC after this time interval, which is in 10ms ticks. Default value: 10

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
maxbridgecollision	<Integer>	Read-write	Maximum bridge collision for loop detection . Default value: 20
bdggrpproxyarp	<String>	Read-write	Set/reset proxy ARP in bridge group deployment. Default value: ENABLED Possible values = ENABLED, DISABLED
bdgsetting	<String>	Read-write	Bridging settings for C2C behavior. If enabled, each PE will learn MAC entries independently. Otherwise, when L2 mode is ON, learned MAC entries on a PE will be broadcasted to all other PEs. Default value: DISABLED Possible values = ENABLED, DISABLED
garponvridintf	<String>	Read-write	Send GARP messagess on VRID-configured interfaces upon failover . Default value: ENABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ENABLED, DISABLED
macmodefwdmypkt	<String>	Read-write	Allows MAC mode vserver to pick and forward the packets even if it is destined to Citrix ADC owned VIP. Default value: DISABLED Possible values = ENABLED, DISABLED
usemymac	<String>	Read-write	Use Citrix ADC MAC for all outgoing packets. Default value: DISABLED Possible values = ENABLED, DISABLED
proxyarp	<String>	Read-write	Proxies the ARP as Citrix ADC MAC for FreeBSD. Default value: ENABLED Possible values = ENABLED, DISABLED
garpreply	<String>	Read-write	Set/reset REPLY form of GARP .

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: DISABLED Possible values = ENABLED, DISABLED
mbfinstlearning	<String>	Read-write	Enable instant learning of MAC changes in MBF mode. Default value: DISABLED Possible values = ENABLED, DISABLED
rstintfonhafo	<String>	Read-write	Enable the reset interface upon HA failover. Default value: DISABLED Possible values = ENABLED, DISABLED
skipproxyingbsdtrafficc	<String>	Read-write	Control source parameters (IP and Port) for FreeBSD initiated traffic. If Enabled, source parameters are retained. Else proxy the source parameters based on next hop.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: DISABLED Possible values = ENABLED, DISABLED
returntoethernetsender	<String>	Read-write	Return to ethernet sender. Default value: DISABLED Possible values = ENABLED, DISABLED
stopmacmoveupdate	<String>	Read-write	Stop Update of server mac change to NAT sessions. Default value: DISABLED Possible values = ENABLED, DISABLED
bridgeagetimeout	<Integer>	Read-write	Time-out value for the bridge table entries, in seconds. The new value applies only to the entries that are dynamically learned after the new value is set. Previously existing bridge table entries expire after the previously configured time-out value.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: 300 Minimum value = 60 Maximum value = 300
usenetprofilebsdtraffic	<String>	Read-write	Control source parameters (IP and Port) for FreeBSD initiated traffic. If enabled proxy the source parameters based on netprofile source ip. If netprofile does not have ip configured, then it will continue to use NSIP as earlier. Default value: DISABLED Possible values = ENABLED, DISABLED
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- UPDATE
- UNSET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/l2param **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"l2param":{

"mbfpeermacupdate":<Integer_value>,

"maxbridgecollision":<Integer_value>,

"bdggrpproxyarp":<String_value>,
```

```
"bdgsetting":<String_value>,

"garponvridintf":<String_value>,

"macmodefwdmypkt":<String_value>,

"usemymac":<String_value>,

"proxyarp":<String_value>,

"garpreply":<String_value>,

"mbfinstlearning":<String_value>,

"rstintfonhafo":<String_value>,

"skipproxyingbsdtraffic":<String_value>,

"returntoethernetsender":<String_value>,

"stopmacmoveupdate":<String_value>,

"bridgeagetimeout":<Integer_value>,

"usenetprofilebsdtraffic":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/l2param? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"l2param":{

"mbfpeermacupdate":true,

"maxbridgecollision":true,

"bdggrpproxyarp":true,

"bdgsetting":true,

"garponvridintf":true,

"macmodefwdmypkt":true,

"usemymac":true,

"proxyarp":true,

"garpreply":true,

"mbfinstlearning":true,

"rstintfonhafo":true,

"skipproxyingbsdtraffic":true,

"returntoethernetsender":true,

"stopmacmoveupdate":true,

"bridgeagetimeout":true,

"usenetprofilebsdtraffic":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/l2param **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "l2param": [ {

"maxbridgecollision":<Integer_value>,

"mbfpeermacupdate":<Integer_value>,

"bdggrpproxyarp":<String_value>,

"bdgsetting":<String_value>,

"garponvridintf":<String_value>,

"macmodefwdmypkt":<String_value>,

"usemymac":<String_value>,

"proxyarp":<String_value>,

"garpreply":<String_value>,

"mbfinstlearning":<String_value>,

"rstintfonhafo":<String_value>,
```

```
"skipproxyingbsdtraffic":<String_value>,

"returntoethernetsender":<String_value>,

"stopmacmoveupdate":<String_value>,

"bridgeagetimeout":<Integer_value>,

"usenetprofilebsdtraffic":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

l3param

Configuration for Layer 3 related parameter resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
srcnat	<String>	Read-write	Perform NAT if only the source is in the private network. Default value: ENABLED Possible values = ENABLED, DISABLED
icmpgenratethreshold	<Integer>	Read-write	NS generated ICMP pkts per 10ms rate threshold. Default value: 100
overridernat	<String>	Read-write	USNIP/USIP settings override RNAT

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			settings for configured service/virtual server traffic.. . Default value: DISABLED Possible values = ENABLED, DISABLED
dropdfflag	<String>	Read-write	Enable dropping the IP DF flag. Default value: DISABLED Possible values = ENABLED, DISABLED
miproundrobin	<String>	Read-write	Enable round robin usage of mapped IPs. Default value: ENABLED Possible values = ENABLED, DISABLED
externalloopback	<String>	Read-write	Enable external loopback. Default value: DISABLED Possible values = ENABLED, DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
tnlpmtuwoconn	<String>	Read-write	Enable/Disable learning PMTU of IP tunnel when ICMP error does not contain connection information. Default value: ENABLED Possible values = ENABLED, DISABLED
usipserverstraypkt	<String>	Read-write	Enable detection of stray server side pkts in USIP mode. Default value: DISABLED Possible values = ENABLED, DISABLED
forwardicmpfragments	<String>	Read-write	Enable forwarding of ICMP fragments. Default value: DISABLED Possible values = ENABLED, DISABLED
dropipfragments	<String>	Read-write	Enable dropping of IP fragments. Default value: DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ENABLED, DISABLED
acllogtime	<Integer>	Read-write	Parameter to tune acl logging time. Default value: 5000
implicitaclallow	<String>	Read-write	Do not apply ACLs for internal ports. Default value: ENABLED Possible values = ENABLED, DISABLED
dynamicrouting	<String>	Read-write	Enable/Disable Dynamic routing on partition. This configuration is not applicable to default partition. Default value: DISABLED Possible values = ENABLED, DISABLED
ipv6dynamicrouting	<String>	Read-write	Enable/Disable IPv6 Dynamic routing. Default value: DISABLED Possible values = ENABLED, DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
allowclasseipv4	<String>	Read-write	Enable/Disable IPv4 Class E address clients. Default value: DISABLED Possible values = ENABLED, DISABLED
implicitpbr	<String>	Read-write	Enable/Disable Policy Based Routing for control packets. Default value: DISABLED Possible values = ENABLED, DISABLED
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- UPDATE
- UNSET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/l3param **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"l3param":{

"srcnat":<String_value>,

"icmpgenratethreshold":<Integer_value>,

"overridernat":<String_value>,

"dropdfflag":<String_value>,

"miproundrobin":<String_value>,

"externalloopback":<String_value>,
```

```
"tnlpmtuwoconn":<String_value>,

"usipserverstraypkt":<String_value>,

"forwardicmpfragments":<String_value>,

"dropipfragments":<String_value>,

"acllogtime":<Integer_value>,

"implicitaclallow":<String_value>,

"dynamicrouting":<String_value>,

"ipv6dynamicrouting":<String_value>,

"allowclasseipv4":<String_value>,

"implicitpbr":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/l3param? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"l3param":{

"srcnat":true,
```

```
"icmpgenratethreshold":true,

"overridernat":true,

"dropdfflag":true,

"miproundrobin":true,

"externalloopback":true,

"tnlpmtuwoconn":true,

"usipserverstraypkt":true,

"forwardicmpfragments":true,

"dropipfragments":true,

"acllogtime":true,

"implicitaclallow":true,

"dynamicrouting":true,

"ipv6dynamicrouting":true,

"allowclasseipv4":true,

"implicitpbr":true

}}
```


Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/l3param **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "l3param": [ {

"srcnat":<String_value>,

"icmpgenratethreshold":<Integer_value>,

"overridernat":<String_value>,

"dropdfflag":<String_value>,

"miproundrobin":<String_value>,

"externalloopback":<String_value>,

"tnlpmtuwoconn":<String_value>,

"usipserverstraypkt":<String_value>,

"forwardicmpfragments":<String_value>,

"dropipfragments":<String_value>,

"acllogtime":<Integer_value>,

"implicitaclallow":<String_value>,

"dynamicrouting":<String_value>,

"ipv6dynamicrouting":<String_value>,
```

```
"allowclasseipv4":<String_value>,

"implicitpbr":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

l4param

Configuration for Layer 4 related parameter resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
l2connmethod	<String>	Read-write	Layer 2 connection method based on the combination of channel number, MAC address and VLAN. It is tuned with l2conn param of lb vserver. If l2conn of lb vserver is ON then method specified here will be used to identify a connection in addition to the 4-tuple (<source IP>:<source port>::<destination IP>:<destination port>). Default value: MacVlanChannel

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = Channel, Vlan, VlanChannel, Mac, MacChannel, MacVlan, MacVlanChannel
l4switch	<String>	Read-write	In L4 switch topology, always clients and servers are on the same side. Enable l4switch to allow such connections. Default value: DISABLED Possible values = ENABLED, DISABLED
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- UPDATE
- UNSET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/l4param **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"l4param":{

"l2connmethod":<String_value>,

"l4switch":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/l4param? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"l4param":{

"l2connmethod":true,

"l4switch":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/l4param **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "l4param": [ {

"l2connmethod":<String_value>,

"l4switch":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

lacp

Configuration for Link aggregation control protocol resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
syspriority	<Integer>	Read-write	Priority number that determines which peer device of an LACP LA channel can have control over the LA channel. This parameter is globally applied to all LACP channels on the Citrix ADC. The lower the number, the higher the priority. Default value: 32768 Minimum value = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum value = 65535
ownernode	<Integer>	Read-write	The owner node in a cluster for which we want to set the lacp priority. Owner node can vary from 0 to 31. Ownernode value of 254 is used for Cluster. Default value: 255
devicename	<String>	Read-only	Name of the channel.
mac	<String>	Read-only	LACP system MAC.
flags	<Integer>	Read-only	Flags of this channel.
lacpkey	<Integer>	Read-only	LACP key of this channel.
clustersyspriority	<Integer>	Read-only	LACP system (Cluster) priority.
clustermac	<String>	Read-only	LACP system (Cluster) mac.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- UPDATE
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/lacp **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"lacp":{

<b>"syspriority":<Integer_value>,

</b>"ownernode":<Integer_value>
```

```
}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/lacp **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/lacp? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/lacp? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of lacp resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/lacp? **view=summary**

Use this query-parameter to get the summary output of lacp resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/lacp? **pagesize=#no;pageno=#no**

Use this query-parameter to get the lacp resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "lacp": [ {

"ownernode":<Integer_value>,

"devicename":<String_value>,

"syspriority":<Integer_value>,

"mac":<String_value>,

"flags":<Integer_value>,

"lacpkey":<Integer_value>,

"clustersyspriority":<Integer_value>,

"clustermac":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/lacp/ ownernode_value<Integer> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/lacp/ ownernode_value<Integer> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/lacp/ ownernode_value<Integer> ? **view=summary**

Use this query-parameter to get the summary output of lacp resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lacp": [ {

"ownernode":<Integer_value>,

"devicename":<String_value>,

"syspriority":<Integer_value>,

"mac":<String_value>,

"flags":<Integer_value>,

"lacpkey":<Integer_value>,

"clustersyspriority":<Integer_value>,

"clustermac":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/lacp? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "lacp": [ { "__count": "#no"} ] }
```

linkset

Configuration for link set resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
id	<String>	Read-write	Unique identifier for the linkset. Must be of the form LS/x, where x can be an integer from 1 to 32.
ifnum	<String>	Read-only	The interfaces to be bound to the linkset.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/linkset

HTTP Method: POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"linkset":{

<b>"id":<String_value>

</b>}}
```

Response:

HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/linkset/ id_value<String>

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/linkset

Query-parameters:

attrs

http:// <netscaler-ip-address> /nitro/v1/config/linkset? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter

http:// <netscaler-ip-address> /nitro/v1/config/linkset? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of linkset resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view

http:// <netscaler-ip-address> /nitro/v1/config/linkset? **view=summary**

Use this query-parameter to get the summary output of linkset resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination

http:// <netscaler-ip-address> /nitro/v1/config/linkset? **pagesize=#no;pageno=#no**

Use this query-parameter to get the linkset resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "linkset": [ {

"id":<String_value>,

"ifnum":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/linkset/ id_value<String>

Query-parameters:

attrs

http:// <netscaler-ip-address> /nitro/v1/config/linkset/ id_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view

http:// <netscaler-ip-address> /nitro/v1/config/linkset/ id_value<String> ? **view=summary**

Use this query-parameter to get the summary output of linkset resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "linkset": [ {

"id":<String_value>,

"ifnum":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/linkset? **count=yes**

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "linkset": [ { "__count": "#no"} ] }
```

linkset_binding

Binding object which returns the resources bound to linkset.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
id	<String>	Read-write	ID of the linkset for which to display information. If an ID is not provided, the display includes information about all linksets that are available in the cluster.
linkset_interface_binding	<linkset_interface_binding[]>	Read-only	interface that can be bound to linkset.
linkset_channel_binding	<linkset_channel_binding[]>	Read-only	channel that can be bound to linkset.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/linkset_binding/ id_value<String>

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "linkset_binding": [ {

"id":<String_value>,

"linkset_interface_binding":<linkset_interface_binding[]_value>,

"linkset_channel_binding":<linkset_channel_binding[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/linkset_binding

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters:

bulkbindings

http:// <netscaler-ip-address> /nitro/v1/config/linkset_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "linkset_binding": [ {

"id":<String_value>,

"linkset_interface_binding":<linkset_interface_binding[]_value>,

"linkset_channel_binding":<linkset_channel_binding[]_value>

}]}
```

linkset_channel_binding

Binding object showing the channel that can be bound to linkset.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ifnum	<String>	Read-write	The interfaces to be bound to the linkset.
id	<String>	Read-write	ID of the linkset to which to bind the interfaces.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/linkset_channel_binding

HTTP Method: PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"linkset_channel_binding":{

<b>"id":<String_value>,

</b><b>"ifnum":<String_value></b>

}}
```

Response:

HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/linkset_channel_binding/ id_value<String>

Query-parameters:

args

http:// <netscaler-ip-address> /nitro/v1/config/linkset_channel_binding/ id_value<String> ? **args= ifnum:<String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/linkset_channel_binding/ id_value<String>

Query-parameters:

filter

http:// <netscaler-ip-address> /nitro/v1/config/linkset_channel_binding/ id_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of linkset_channel_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination

http:// <netscaler-ip-address> /nitro/v1/config/linkset_channel_binding/ id_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the linkset_channel_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "linkset_channel_binding": [ {

"ifnum":<String_value>,

"id":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/linkset_channel_binding

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters:

bulkbindings

http:// <netscaler-ip-address> /nitro/v1/config/linkset_channel_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "linkset_channel_binding": [ {

"ifnum":<String_value>,

"id":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/linkset_channel_binding/ id_value<String> ? **count=yes**

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"linkset_channel_binding": [ { "__count": "#no"} ] }
```

linkset_interface_binding

Binding object showing the interface that can be bound to linkset.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ifnum	<String>	Read-write	The interfaces to be bound to the linkset.
id	<String>	Read-write	ID of the linkset to which to bind the interfaces.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of

creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/linkset_interface_binding

HTTP Method: PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"linkset_interface_binding":{

<b>"id":<String_value>,

</b><b>"ifnum":<String_value></b>

}}
```

Response:

HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/linkset_interface_binding/ id_value<String>

Query-parameters:

args

http:// <netscaler-ip-address> /nitro/v1/config/linkset_interface_binding/ id_value<String> ? **args= ifnum:<String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/linkset_interface_binding/ id_value<String>

Query-parameters:

filter

http:// <netscaler-ip-address> /nitro/v1/config/linkset_interface_binding/ id_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of linkset_interface_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination

http:// <netscaler-ip-address> /nitro/v1/config/linkset_interface_binding/ id_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the linkset_interface_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "linkset_interface_binding": [ {

"ifnum":<String_value>,

"id":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/linkset_interface_binding

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters:

bulkbindings

http:// <netscaler-ip-address> /nitro/v1/config/linkset_interface_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "linkset_interface_binding": [ {

"ifnum":<String_value>,

"id":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/linkset_interface_binding/ id_value<String> ? **count=yes**

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"linkset_interface_binding": [ { "__count": "#no"} ] }
```

mapbmr

Configuration for MAP-T Basic Mapping rule resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the Basic Mapping Rule. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			be changed after the MAP Basic Mapping Rule is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "add network MapBmr bmr1 -natprefix 2005::/64 -EAbitLength 16 -psidoffset 6 -portsharingratio 8"). The Basic Mapping Rule information allows a MAP BR to determine source IPv4 address from the IPv6 packet sent from MAP CE device. Also it allows to determine destination IPv6 address of MAP CE before sending packets to MAP CE. Minimum length = 1 Maximum length = 127

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ruleipv6prefix	<String>	Read-write	IPv6 prefix of Customer Edge(CE) device.MAP-T CE will send ipv6 packets with this ipv6 prefix as source ipv6 address prefix.
psidoffset	<Integer>	Read-write	Start bit position of Port Set Identifier(PSID) value in Embedded Address (EA) bits. Default value: 6 Minimum value = 1 Maximum value = 15
eabitlength	<Integer>	Read-write	The Embedded Address (EA) bit field encodes the CE-specific IPv4 address and port information. The EA bit field, which is unique for a given Rule IPv6 prefix. Default value: 16 Minimum value = 2 Maximum value = 47
psidlength	<Integer>	Read-write	Length of Port Set IdentifierPort Set Identifier(PSID) in

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Embedded Address (EA) bits. Default value: 8 Minimum value = 1 Maximum value = 16
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/mapbmr **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"mapbmr":{

<b>"name":<String_value>,

</b><b>"ruleipv6prefix":<String_value>,

</b>"psidoffset":<Integer_value>,

"eabitlength":<Integer_value>,

"psidlength":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/mapbmr/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/mapbmr **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/mapbmr? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/mapbmr? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of mapbmr resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/mapbmr? **view=summary**

Use this query-parameter to get the summary output of mapbmr resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/mapbmr? **pagesize=#no;pageno=#no**

Use this query-parameter to get the mapbmr resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "mapbmr": [ {

"name":<String_value>,

"ruleipv6prefix":<String_value>,

"eabitlength":<Integer_value>,

"psidoffset":<Integer_value>,

"psidlength":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/mapbmr/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/mapbmr/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/mapbmr/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of mapbmr resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "mapbmr": [ {

"name":<String_value>,

"ruleipv6prefix":<String_value>,

"eabitlength":<Integer_value>,

"psidoffset":<Integer_value>,

"psidlength":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/mapbmr? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "mapbmr": [ { "__count": "#no"} ] }
```

mapbmr_binding

Binding object which returns the resources bound to mapbmr.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the Basic Mapping Rule. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the MAP Basic Mapping Rule is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			quotation marks (for example, "add network MapBmr bmr1 -natprefix 2005::/64 -EAbitLength 16 -psidoffset 6 -portsharingratio 8"). The Basic Mapping Rule information allows a MAP BR to determine source IPv4 address from the IPv6 packet sent from MAP CE device. Also it allows to determine destination IPv6 address of MAP CE before sending packets to MAP CE. Minimum length = 1 Maximum length = 127
mapbmr_bmrv4network_binding	<mapbmr_bmrv4network_binding[]>	Read-only	bmrv4network that can be bound to mapbmr.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/mapbmr_binding/ name_value<String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "mapbmr_binding": [ {

"name":<String_value>,

"mapbmr_bmrv4network_binding":<mapbmr_bmrv4network_binding[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/mapbmr_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/mapbmr_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "mapbmr_binding": [ {

"name":<String_value>,
```

```
"mapbmr_bmrv4network_binding":<mapbmr_bmrv4network_binding[]_value>

}]}
```

mapbmr_bmrv4network_binding

Binding object showing the bmrv4network that can be bound to mapbmr.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
netmask	<String>	Read-write	Subnet mask for the IPv4 address specified in the Network parameter.
network	<String>	Read-write	IPv4 NAT address range of Customer Edge (CE). Minimum length = 1
name	<String>	Read-write	Name for the Basic Mapping Rule. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the MAP Basic Mapping Rule is created. The following

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "add network MapBmr bmr1 -natprefix 2005::/64 -EAbitLength 16 -psidoffset 6 -portsharingratio 8"). The Basic Mapping Rule information allows a MAP BR to determine source IPv4 address from the IPv6 packet sent from MAP CE device. Also it allows to determine destination IPv6 address of MAP CE before sending packets to MAP CE. Minimum length = 1 Maximum length = 127
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/mapbmr_bmrv4network_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"mapbmr_bmrv4network_binding":{

<b>"name":<String_value>,

</b><b>"network":<String_value>,

</b>"netmask":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/mapbmr_bmrv4network_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ mapbmr_bmrv4network_binding/ name_value<String> ? **args= network:<String_value>, netmask: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/mapbmr_bmrv4network_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ mapbmr_bmrv4network_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of mapbmr_bmrv4network_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/mapbmr_bmrv4network_binding/name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the mapbmr_bmrv4network_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "mapbmr_bmrv4network_binding": [ {

"netmask":<String_value>,

"network":<String_value>,

"name":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/mapbmr_bmrv4network_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/mapbmr_bmrv4network_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "mapbmr_bmrv4network_binding": [ {

"netmask":<String_value>,

"network":<String_value>,

"name":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/mapbmr_bmrv4network_binding/name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"mapbmr_bmrv4network_binding": [ { "__count": "#no"} ] }
```

mapdmr

Configuration for MAP-T Default Mapping rule resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the Default Mapping Rule. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the MAP Default Mapping Rule is created. The following requirement applies only to the Citrix ADC CLI: If the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			name includes one or more spaces, enclose the name in double or single quotation marks (for example, "add network MapDmr map1 -BRIpv6Prefix 2003::/96"). Default Mapping Rule (DMR) is defined in terms of the IPv6 prefix advertised by one or more BRs, which provide external connectivity. A typical MAP-T CE will install an IPv4 default route using this rule. A BR will use this rule when translating all outside IPv4 source addresses to the IPv6 MAP domain. Minimum length = 1 Maximum length = 127
bripv6prefix	<String>	Read-write	IPv6 prefix of Border Relay (Citrix ADC) device.MAP-T CE will send ipv6 packets to this ipv6 prefix.The DMR IPv6 prefix length

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			SHOULD be 64 bits long by default and in any case MUST NOT exceed 96 bits.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/mapdmr **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"mapdmr":{

<b>"name":<String_value>,

</b><b>"bripv6prefix":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/mapdmr/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/mapdmr **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/mapdmr? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/mapdmr? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of mapdmr resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/mapdmr? **view=summary**

Use this query-parameter to get the summary output of mapdmr resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/mapdmr? **pagesize=#no;pageno=#no**

Use this query-parameter to get the mapdmr resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "mapdmr": [ {

"name":<String_value>,
```

```
"bripv6prefix":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/mapdmr/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/mapdmr/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/mapdmr/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of mapdmr resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "mapdmr": [ {

"name":<String_value>,

"bripv6prefix":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/mapdmr? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "mapdmr": [ { "__count": "#no"} ] }
```

mapdomain

Configuration for MAP-T Map Domain resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the MAP Domain. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the MAP Domain is created . The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "add network MapDomain map1"). Minimum length = 1 Maximum length = 127
mapdmrname	<String>	Read-write	Default Mapping rule name.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/mapdomain **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"mapdomain":{

<b>"name":<String_value>,

</b><b>"mapdmrname":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/mapdomain/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/mapdomain **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/mapdomain? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/mapdomain? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of mapdomain resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/mapdomain? **view=summary**

Use this query-parameter to get the summary output of mapdomain resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/mapdomain? **pagesize=#no;pageno=#no**

Use this query-parameter to get the mapdomain resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "mapdomain": [ {

"name":<String_value>,

"mapdmrname":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/mapdomain/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/mapdomain/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/mapdomain/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of mapdomain resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "mapdomain": [ {

"name":<String_value>,

"mapdmrname":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

```
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/mapdomain? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "mapdomain": [ { "__count": "#no"} ] }
```

mapdomain_binding

Binding object which returns the resources bound to mapdomain.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the MAP Domain. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			(#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the MAP Domain is created . The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "add network MapDomain map1"). Minimum length = 1 Maximum length = 127
mapdomain_mapbmr_binding	<mapdomain_mapbmr_binding[]>	Read-only	mapbmr that can be bound to mapdomain.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/mapdomain_binding/ name_value<String>
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "mapdomain_binding": [ {

"name":<String_value>,

"mapdomain_mapbmr_binding":<mapdomain_mapbmr_binding[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/mapdomain_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/mapdomain_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "mapdomain_binding": [ {

"name":<String_value>,

"mapdomain_mapbmr_binding":<mapdomain_mapbmr_binding[]_value>

}]}
```

mapdomain_mapbmr_binding

Binding object showing the mapbmr that can be bound to mapdomain.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the MAP Domain. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the MAP Domain is created . The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "add network MapDomain map1"). Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum length = 127
mapbmrname	<String>	Read-write	Basic Mapping rule name.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT
- ADD
- DELETE

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/mapdomain_mapbmr_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"mapdomain_mapbmr_binding":{

<b>"name":<String_value>,

</b><b>"mapbmrname":<String_value></b>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/mapdomain_mapbmr_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ mapdomain_mapbmr_binding/ name_value<String> ? **args= mapbmrname:<String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/mapdomain_mapbmr_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ mapdomain_mapbmr_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of mapdomain_mapbmr_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/mapdomain_mapbmr_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the mapdomain_mapbmr_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "mapdomain_mapbmr_binding": [ {

"name":<String_value>,

"mapbmrname":<String_value>
```

```
}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/mapdomain_mapbmr_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/mapdomain_mapbmr_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "mapdomain_mapbmr_binding": [ {

"name":<String_value>,

"mapbmrname":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/mapdomain_mapbmr_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"mapdomain_mapbmr_binding": [ { "__count": "#no"} ] }
```

nat64

Configuration for nat64 config resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the NAT64 rule. Must begin with a letter, number, or the underscore character (_), and can consist of letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			(=), colon (:), and underscore characters. Cannot be changed after the rule is created. Choose a name that helps identify the NAT64 rule. Minimum length = 1
acl6name	<String>	Read-write	Name of any configured ACL6 whose action is ALLOW. IPv6 Packets matching the condition of this ACL6 rule and destination IP address of these packets matching the NAT64 IPv6 prefix are considered for NAT64 translation. Minimum length = 1
netprofile	<String>	Read-write	Name of the configured netprofile. The Citrix ADC selects one of the IP address in the netprofile as the source IP address of the translated IPv4 packet to be sent to the IPv4 server. Minimum length = 1 Maximum length = 127

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- UPDATE
- UNSET
- DELETE
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/nat64 **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nat64":{

<b>"name":<String_value>,

</b><b>"acl6name":<String_value>,

</b>"netprofile":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/nat64 **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nat64":{

<b>"name":<String_value>,

</b>"acl6name":<String_value>,

"netprofile":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/nat64? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nat64":{

<b>"name":<String_value>,

</b>"netprofile":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/nat64/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/nat64 **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/nat64? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/nat64? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of nat64 resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/nat64? **view=summary**

Use this query-parameter to get the summary output of nat64 resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/nat64? **pagesize=#no;pageno=#no**

Use this query-parameter to get the nat64 resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nat64": [ {

"name":<String_value>,

"acl6name":<String_value>,

"netprofile":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/nat64/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/nat64/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/nat64/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of nat64 resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "nat64": [ {

"name":<String_value>,

"acl6name":<String_value>,

"netprofile":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/nat64? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nat64": [ { "__count": "#no"} ] }
```

nat64param

Configuration for NAT64 parameter resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
td	<Integer>	Read-write	Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0. Default value: 0 Minimum value = 0 Maximum value = 4094
nat64ignoretos	<String>	Read-write	Ignore TOS. Default value: NO Possible values = YES, NO
nat64zerochecksum	<String>	Read-write	Calculate checksum for UDP packets with zero checksum. Default value: ENABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ENABLED, DISABLED
nat64v6mtu	<Integer>	Read-write	MTU setting for the IPv6 side. If the incoming IPv4 packet greater than this, either fragment or send icmp need fragmentation error. Default value: 1280 Minimum value = 1280 Maximum value = 9216
nat64fragheader	<String>	Read-write	When disabled, translator will not insert IPv6 fragmentation header for non fragmented IPv4 packets. Default value: ENABLED Possible values = ENABLED, DISABLED
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/nat64param **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nat64param":{

"td":<Integer_value>,

"nat64ignoretos":<String_value>,

"nat64zerochecksum":<String_value>,

"nat64v6mtu":<Integer_value>,

"nat64fragheader":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/nat64param? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nat64param":{

"td":<Integer_value>,

"nat64ignoretos":true,

"nat64zerochecksum":true,

"nat64v6mtu":true,
```

```
"nat64fragheader":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/nat64param **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/nat64param? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/nat64param? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of nat64param resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/nat64param? **view=summary**

Use this query-parameter to get the summary output of nat64param resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/nat64param? **pagesize=#no;pageno=#no**

Use this query-parameter to get the nat64param resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nat64param": [ {

"td":<Integer_value>,

"nat64ignoretos":<String_value>,

"nat64zerochecksum":<String_value>,

"nat64v6mtu":<Integer_value>,

"nat64fragheader":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/nat64param/ td_value<Integer> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/nat64param/ td_value<Integer> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/nat64param/ td_value<Integer> ? **view=summary**

Use this query-parameter to get the summary output of nat64param resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "nat64param": [ {

"td":<Integer_value>,

"nat64ignoretos":<String_value>,

"nat64zerochecksum":<String_value>,

"nat64v6mtu":<Integer_value>,

"nat64fragheader":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/nat64param? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nat64param": [ { "__count": "#no"} ] }
```

nd6

Configuration for nd6 resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
neighbor	<String>	Read-write	Link-local IPv6 address of the adjacent network device to add to the ND6 table.
mac	<String>	Read-write	MAC address of the adjacent network device.
ifnum	<String>	Read-write	Interface through which the adjacent network device is available, specified in slot/port notation (for example, 1/3). Use spaces to separate multiple entries.
vlan	<Integer>	Read-write	Integer value that uniquely identifies

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			the VLAN on which the adjacent network device exists. Minimum value = 1 Maximum value = 4094
vxlan	<Integer>	Read-write	ID of the VXLAN on which the IPv6 address of this ND6 entry is reachable. Minimum value = 1 Maximum value = 16777215
vtep	<String>	Read-write	IP address of the VXLAN tunnel endpoint (VTEP) through which the IPv6 address of this ND6 entry is reachable. Minimum length = 1
td	<Integer>	Read-write	Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0. Minimum value = 0

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum value = 4094
nodeid	<Integer>	Read-write	Unique number that identifies the cluster node. Minimum value = 0 Maximum value = 31
state	<String>	Read-only	ND6 state. Default value: REACHABLE Possible values = INCOMPLETE, REACHABLE, STALE, DELAY, PROBE
timeout	<Integer>	Read-only	Time elapsed.
flags	<Integer>	Read-only	flag for static/ permanent entry.
controlplane	<Boolean>	Read-only	This nd6 entry is populated by a control plane protocol.
channel	<Integer>	Read-only	The tunnel that is bound to a netbridge.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- CLEAR
- DELETE
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/nd6 **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nd6":{

<b>"neighbor":<String_value>,

</b><b>"mac":<String_value>,

</b>"ifnum":<String_value>,

"vlan":<Integer_value>,

"vxlan":<Integer_value>,

"vtep":<String_value>,

"td":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

CLEAR

URL: http:// <netscaler-ip-address> /nitro/v1/config/nd6? **action=clear HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nd6":{

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/nd6/ neighbor_value<String> **Query-parameters: args=vlan: <Integer_value> ,vxlan: <Integer_value> ,td: <Integer_value>**
get (all)
URL: http:// <netscaler-ip-address> /nitro/v1/config/nd6 **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/nd6? **args=neighbor: <String_value> ,td: <Integer_value> ,nodeid: <Integer_value>**

Use this query-parameter to get nd6 resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/config/nd6? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/nd6? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of nd6 resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/nd6? **view=summary**

Use this query-parameter to get the summary output of nd6 resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/nd6? **pagesize=#no;pageno=#no**

Use this query-parameter to get the nd6 resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nd6": [ {

neighbor:<String_value>,td:<Integer_value>,nodeid:<Integer_value>"mac":<St
ring_value>,

"state":<String_value>,

"timeout":<Integer_value>,

"ifnum":<String_value>,

"vlan":<Integer_value>,

"vxlan":<Integer_value>,

"vtep":<String_value>,

"flags":<Integer_value>,

"controlplane":<Boolean_value>,

"channel":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

count

URL: http:// <netscaler-ip-address> /nitro/v1/config/nd6? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nd6": [ { "__count": "#no"} ] }
```

nd6ravariables

Configuration for nd6 Router Advertisment configuration variables resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
vlan	<Integer>	Read-write	The VLAN number. Minimum value = 1 Maximum value = 4094
ceaserouteradv	<String>	Read-write	Cease router advertisements on this vlan. Default value: NO Possible values = YES, NO
sendrouteradv	<String>	Read-write	whether the router sends periodic RAs and responds to Router Solicitations. Default value: NO

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = YES, NO
srclinklayeraddroption	<String>	Read-write	Include source link layer address option in RA messages. Default value: YES Possible values = YES, NO
onlyunicastrtadvresponse	<String>	Read-write	Send only Unicast Router Advertisements in respond to Router Solicitations. Default value: NO Possible values = YES, NO
managedaddrconfig	<String>	Read-write	Value to be placed in the Managed address configuration flag field. Default value: NO Possible values = YES, NO
otheraddrconfig	<String>	Read-write	Value to be placed in the Other configuration flag field. Default value: NO Possible values = YES, NO

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
currhoplimit	<Integer>	Read-write	Current Hop limit. Default value: 64 Minimum value = 0 Maximum value = 255
maxrtadvinterval	<Integer>	Read-write	Maximum time allowed between unsolicited multicast RAs, in seconds. Default value: 600 Minimum value = 4 Maximum value = 1800
minrtadvinterval	<Integer>	Read-write	Minimum time interval between RA messages, in seconds. Default value: 198 Minimum value = 3 Maximum value = 1350
linkmtu	<Integer>	Read-write	The Link MTU. Default value: 0 Minimum value = 0 Maximum value = 1500
reachabletime	<Integer>	Read-write	Reachable time, in milliseconds.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: 0 Minimum value = 0 Maximum value = 3600000
retranstime	<Integer>	Read-write	Retransmission time, in milliseconds. Default value: 0
defaultlifetime	<Integer>	Read-write	Default life time, in seconds. Default value: 1800 Minimum value = 0 Maximum value = 9000
lastrtadvtime	<Integer>	Read-only	Last RA sent timestamp.
nextrtadvdelay	<Integer>	Read-only	Next RA delay.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/nd6ravariables **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nd6ravariables":{

<b>"vlan":<Integer_value>,

</b>"ceaserouteradv":<String_value>,

"sendrouteradv":<String_value>,
```

```
"srclinklayeraddroption":<String_value>,

"onlyunicastrtadvresponse":<String_value>,

"managedaddrconfig":<String_value>,

"otheraddrconfig":<String_value>,

"currhoplimit":<Integer_value>,

"maxrtadvinterval":<Integer_value>,

"minrtadvinterval":<Integer_value>,

"linkmtu":<Integer_value>,

"reachabletime":<Integer_value>,

"retranstime":<Integer_value>,

"defaultlifetime":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/nd6ravariables? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nd6ravariables":{

<b>"vlan":<Integer_value>,

</b>"ceaserouteradv":true,

"sendrouteradv":true,

"srclinklayeraddroption":true,

"onlyunicastrtadvresponse":true,

"managedaddrconfig":true,

"otheraddrconfig":true,

"currhoplimit":true,

"maxrtadvinterval":true,

"minrtadvinterval":true,

"linkmtu":true,

"reachabletime":true,

"retranstime":true,

"defaultlifetime":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/nd6ravariables **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/nd6ravariables? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/nd6ravariables? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of nd6ravariables resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/nd6ravariables? **view=summary**

Use this query-parameter to get the summary output of nd6ravariables resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/nd6ravariables? **pagesize=#no;pageno=#no**

Use this query-parameter to get the nd6ravariables resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nd6ravariables": [ {

"vlan":<Integer_value>,

"ceaserouteradv":<String_value>,

"sendrouteradv":<String_value>,
```

```
"srclinklayeraddroption":<String_value>,

"onlyunicastrtadvresponse":<String_value>,

"managedaddrconfig":<String_value>,

"otheraddrconfig":<String_value>,

"currhoplimit":<Integer_value>,

"maxrtadvinterval":<Integer_value>,

"minrtadvinterval":<Integer_value>,

"linkmtu":<Integer_value>,

"reachabletime":<Integer_value>,

"retranstime":<Integer_value>,

"defaultlifetime":<Integer_value>,

"lastrtadvtime":<Integer_value>,

"nextrtadvdelay":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/nd6ravariables/ vlan_value<Integer> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/nd6ravariables/ vlan_value<Integer> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/nd6ravariables/ vlan_value<Integer> ? **view=summary**

Use this query-parameter to get the summary output of nd6ravariables resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "nd6ravariables": [ {

"vlan":<Integer_value>,

"ceaserouteradv":<String_value>,

"sendrouteradv":<String_value>,

"srclinklayeraddroption":<String_value>,

"onlyunicastrtadvresponse":<String_value>,

"managedaddrconfig":<String_value>,

"otheraddrconfig":<String_value>,

"currhoplimit":<Integer_value>,

"maxrtadvinterval":<Integer_value>,
```

```
"minrtadvinterval":<Integer_value>,

"linkmtu":<Integer_value>,

"reachabletime":<Integer_value>,

"retranstime":<Integer_value>,

"defaultlifetime":<Integer_value>,

"lastrtadvtime":<Integer_value>,

"nextrtadvdelay":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/nd6ravariables? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nd6ravariables": [ { "__count": "#no"} ] }
```

nd6ravariables_binding

Binding object which returns the resources bound to nd6ravariables.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
vlan	<Integer>	Read-write	The VLAN number. Minimum value = 1 Maximum value = 4094
nd6ravariables_onlinkipv6prefix_binding	<nd6ravariables_onlinkipv6prefix_binding[]>	Read-only	onlinkipv6prefix that can be bound to nd6ravariables.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/nd6ravariables_binding/ vlan_value<Integer>
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nd6ravariables_binding": [ {

"vlan":<Integer_value>,

"nd6ravariables_onlinkipv6prefix_binding":<nd6ravariables_onlinkipv6prefix
_binding[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/nd6ravariables_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/nd6ravariables_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nd6ravariables_binding": [ {

"vlan":<Integer_value>,

"nd6ravariables_onlinkipv6prefix_binding":<nd6ravariables_onlinkipv6prefix
_binding[]_value>

}]}
```

nd6ravariables_onlinkipv6prefix_binding

Binding object showing the onlinkipv6prefix that can be bound to nd6ravariables.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
vlan	<Integer>	Read-write	The VLAN number.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum value = 1 Maximum value = 4094
ipv6prefix	<String>	Read-write	Onlink prefixes for RA messages.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT
- ADD
- DELETE

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/nd6ravariables_onlinkipv6prefix_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"nd6ravariables_onlinkipv6prefix_binding":{

<b>"vlan":<Integer_value>,

</b><b>"ipv6prefix":<String_value></b>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/nd6ravariables_onlinkipv6prefix_binding/ vlan_value<Integer> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ nd6ravariables_onlinkipv6prefix_binding/ vlan_value<Integer> ? **args= ipv6prefix:<String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/nd6ravariables_onlinkipv6prefix_binding/ vlan_value<Integer> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ nd6ravariables_onlinkipv6prefix_binding/ vlan_value<Integer> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of nd6ravariables_onlinkipv6prefix_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/nd6ravariables_onlinkipv6prefix_binding/ vlan_value<Integer> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the nd6ravariables_onlinkipv6prefix_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "nd6ravariables_onlinkipv6prefix_binding": [ {

"vlan":<Integer_value>,
```

```
"ipv6prefix":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/nd6ravariables_onlinkipv6prefix_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/nd6ravariables_onlinkipv6prefix_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "nd6ravariables_onlinkipv6prefix_binding": [ {

"vlan":<Integer_value>,

"ipv6prefix":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/nd6ravariables_onlinkipv6prefix_binding/vlan_value<Integer> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"nd6ravariables_onlinkipv6prefix_binding": [ { "__count": "#no"} ] }
```

netbridge

Configuration for network bridge resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	The name of the network bridge.
vxlanvlanmap	<String>	Read-write	The vlan to vxlan mapping to be applied to this netbridge.
_nextgenapiresource	<String>	Read-only	.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- UPDATE
- UNSET
- DELETE
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/netbridge

HTTP Method: POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"netbridge":{

<b>"name":<String_value>,

</b>"vxlanvlanmap":<String_value>

}}
```

Response:

HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/netbridge

HTTP Method: PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"netbridge":{

<b>"name":<String_value>,

</b>"vxlanvlanmap":<String_value>

}}
```

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/netbridge? **action=unset**

HTTP Method: POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"netbridge":{

<b>"name":<String_value>,

</b>"vxlanvlanmap":true

}}
```

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/netbridge/ name_value<String>

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/netbridge

Query-parameters:

attrs

http:// <netscaler-ip-address> /nitro/v1/config/netbridge? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter

http:// <netscaler-ip-address> /nitro/v1/config/netbridge? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of netbridge resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view

http:// <netscaler-ip-address> /nitro/v1/config/netbridge? **view=summary**

Use this query-parameter to get the summary output of netbridge resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination

http:// <netscaler-ip-address> /nitro/v1/config/netbridge? **pagesize=#no;pageno=#no**

Use this query-parameter to get the netbridge resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "netbridge": [ {

"name":<String_value>,

"vxlanvlanmap":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/netbridge/ name_value<String>

Query-parameters:

attrs

http:// <netscaler-ip-address> /nitro/v1/config/netbridge/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view

http:// <netscaler-ip-address> /nitro/v1/config/netbridge/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of netbridge resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "netbridge": [ {

"name":<String_value>,

"vxlanvlanmap":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/netbridge? **count=yes**

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "netbridge": [ { "__count": "#no"} ] }
```

netbridge_binding

Binding object which returns the resources bound to netbridge.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	The name of the network bridge.
netbridge_vlan_binding	<netbridge_vlan_binding[]>	Read-only	vlan that can be bound to netbridge.
netbridge_nsip6_binding	<netbridge_nsip6_binding[]>	Read-only	nsip6 that can be bound to netbridge.
netbridge_nsip_binding	<netbridge_nsip_binding[]>	Read-only	nsip that can be bound to netbridge.
netbridge_iptunnel_binding	<netbridge_iptunnel_binding[]>	Read-only	iptunnel that can be bound to netbridge.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of

creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/netbridge_binding/ name_value<String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "netbridge_binding": [ {

"name":<String_value>,

"netbridge_nsip_binding":<netbridge_nsip_binding[]_value>,

"netbridge_iptunnel_binding":<netbridge_iptunnel_binding[]_value>,
```

```
"netbridge_vlan_binding":<netbridge_vlan_binding[]_value>,

"netbridge_nsip6_binding":<netbridge_nsip6_binding[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/netbridge_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/netbridge_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "netbridge_binding": [ {

"name":<String_value>,

"netbridge_nsip_binding":<netbridge_nsip_binding[]_value>,

"netbridge_iptunnel_binding":<netbridge_iptunnel_binding[]_value>,

"netbridge_vlan_binding":<netbridge_vlan_binding[]_value>,
```

```
"netbridge_nsip6_binding":<netbridge_nsip6_binding[]_value>

}]}
```

netbridge_iptunnel_binding

Binding object showing the iptunnel that can be bound to netbridge.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	The name of the network bridge.
tunnel	<String>	Read-write	The name of the tunnel that is a part of this bridge.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT
- ADD
- DELETE

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/netbridge_iptunnel_binding

HTTP Method: PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"netbridge_iptunnel_binding":{

<b>"name":<String_value>,

</b>"tunnel":<String_value>

}}
```

Response:

HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/netbridge_iptunnel_binding/ name_value<String>

Query-parameters:

args

http:// <netscaler-ip-address> /nitro/v1/config/netbridge_iptunnel_binding/ name_value<String> ? **args=tunnel: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/netbridge_iptunnel_binding/ name_value<String>

Query-parameters:

filter

http:// <netscaler-ip-address> /nitro/v1/config/netbridge_iptunnel_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of netbridge_iptunnel_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination

http:// <netscaler-ip-address> /nitro/v1/config/netbridge_iptunnel_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the netbridge_iptunnel_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "netbridge_iptunnel_binding": [ {

"name":<String_value>,

"tunnel":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/netbridge_iptunnel_binding

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters:

bulkbindings

http:// <netscaler-ip-address> /nitro/v1/config/netbridge_iptunnel_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "netbridge_iptunnel_binding": [ {

"name":<String_value>,

"tunnel":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/netbridge_iptunnel_binding/ name_value<String> ? **count=yes**

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"netbridge_iptunnel_binding": [ { "__count": "#no"} ] }
```

netbridge_nsip6_binding

Binding object showing the nsip6 that can be bound to netbridge.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ipaddress	<String>	Read-write	The subnet that is extended by this network bridge. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	The name of the network bridge.
netmask	<String>	Read-write	The network mask for the subnet.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT
- ADD
- DELETE

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/netbridge_nsip6_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"netbridge_nsip6_binding":{

<b>"name":<String_value>,

</b>"ipaddress":<String_value>,

"netmask":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/netbridge_nsip6_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/netbridge_nsip6_binding/ name_value<String> ? **args=ipaddress: <String_value> ,netmask: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/netbridge_nsip6_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/netbridge_nsip6_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of netbridge_nsip6_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/netbridge_nsip6_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the netbridge_nsip6_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "netbridge_nsip6_binding": [ {

"ipaddress":<String_value>,
```

```
"name":<String_value>,

"netmask":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/netbridge_nsip6_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/netbridge_nsip6_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "netbridge_nsip6_binding": [ {

"ipaddress":<String_value>,

"name":<String_value>,

"netmask":<String_value>

}]}
```

```
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/netbridge_nsip6_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"netbridge_nsip6_binding": [ { "__count": "#no"} ] }
```

netbridge_nsip_binding

Binding object showing the nsip that can be bound to netbridge.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	The name of the network bridge.
ipaddress	<String>	Read-write	The subnet that is extended by this network bridge. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
netmask	<String>	Read-write	The network mask for the subnet.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT
- ADD
- DELETE

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/netbridge_nsip_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"netbridge_nsip_binding":{

<b>"name":<String_value>,

</b>"ipaddress":<String_value>,

"netmask":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/netbridge_nsip_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/netbridge_nsip_binding/ name_value<String> ? **args=ipaddress: <String_value> ,netmask: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/netbridge_nsip_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/netbridge_nsip_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of netbridge_nsip_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/netbridge_nsip_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the netbridge_nsip_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "netbridge_nsip_binding": [ {

"name":<String_value>,

"ipaddress":<String_value>,

"netmask":<String_value>
```

```
}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/netbridge_nsip_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/netbridge_nsip_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "netbridge_nsip_binding": [ {

"name":<String_value>,

"ipaddress":<String_value>,

"netmask":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/netbridge_nsip_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"netbridge_nsip_binding": [ { "__count": "#no"} ] }
```

netbridge_vlan_binding

Binding object showing the vlan that can be bound to netbridge.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	The name of the network bridge.
vlan	<Integer>	Read-write	The VLAN that is extended by this network bridge. Minimum value = 1 Maximum value = 4094

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT
- ADD
- DELETE

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/netbridge_vlan_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"netbridge_vlan_binding":{

<b>"name":<String_value>,

</b>"vlan":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/netbridge_vlan_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/netbridge_vlan_binding/ name_value<String> ? **args=vlan: <Integer_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/netbridge_vlan_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/netbridge_vlan_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of netbridge_vlan_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/netbridge_vlan_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the netbridge_vlan_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "netbridge_vlan_binding": [ {

"name":<String_value>,

"vlan":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/netbridge_vlan_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ netbridge_vlan_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "netbridge_vlan_binding": [ {

"name":<String_value>,

"vlan":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/netbridge_vlan_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"netbridge_vlan_binding": [ { "__count": "#no"} ] }
```

netprofile

Configuration for Network profile resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the net profile. Must begin with a letter, number, or the underscore character (_), and can consist of letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore characters. Cannot be changed after the profile is created. Choose a name that helps identify the net profile.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum length = 1
td	<Integer>	Read-write	Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0. Minimum value = 0 Maximum value = 4094
srcip	<String>	Read-write	IP address or the name of an IP set.
srcippersistency	<String>	Read-write	When the net profile is associated with a virtual server or its bound services, this option enables the Citrix ADC to use the same address, specified in the net profile, to communicate to servers for all sessions initiated from a particular client to the virtual server. Default value: DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ENABLED, DISABLED
overridelsn	<String>	Read-write	USNIP/USIP settings override LSN settings for configured service/virtual server traffic.. . Default value: DISABLED Possible values = ENABLED, DISABLED
mbf	<String>	Read-write	Response will be sent using learnt info if enabled. When creating a netprofile, if you do not set this parameter, the netprofile inherits the global MBF setting (available in the enable ns mode and disable ns mode CLI commands, or in the System > Settings > Configure modes > Configure Modes dialog box). However, you can override this setting after you create the netprofile.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ENABLED, DISABLED
proxyprotocol	<String>	Read-write	Proxy Protocol Action (Enabled/ Disabled). Default value: DISABLED Possible values = ENABLED, DISABLED
proxyprotocoltxversion	<String>	Read-write	Proxy Protocol Version (V1/V2). Default value: V1 Possible values = V1, V2
proxyprotocolaftertls handshake	<String>	Read-write	ADC doesnt look for proxy header before TLS handshake, if enabled. Proxy protocol parsed after TLS handshake. Default value: DISABLED Possible values = ENABLED, DISABLED
badipactionthreshold	<Integer>	Read-write	Number of protocol violation from an IP address before taking action. Default value: 0

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum value = 0 Maximum value = 100000
proxyprotocoltlvoptions	<String[]>	Read-only	Proxy protocol TLV options. Possible values = cert-cn
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of

creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/netprofile **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"netprofile":{

<b>"name":<String_value>,

</b>"td":<Integer_value>,

"srcip":<String_value>,

"srcippersistency":<String_value>,

"overridelsn":<String_value>,

"mbf":<String_value>,

"proxyprotocol":<String_value>,

"proxyprotocoltxversion":<String_value>,
```

```
"proxyprotocolaftertlshandshake":<String_value>,

"badipactionthreshold":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/netprofile/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/netprofile **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"netprofile":{

<b>"name":<String_value>,

</b>"srcip":<String_value>,

"srcippersistency":<String_value>,
```

```
"overridelsn":<String_value>,

"mbf":<String_value>,

"proxyprotocol":<String_value>,

"proxyprotocoltxversion":<String_value>,

"proxyprotocolaftertlshandshake":<String_value>,

"badipactionthreshold":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/netprofile? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"netprofile":{

<b>"name":<String_value>,

</b>"srcip":true,

"srcippersistency":true,

"badipactionthreshold":true,
```

```
"overridelsn":true,

"mbf":true,

"proxyprotocol":true,

"proxyprotocoltxversion":true,

"proxyprotocolaftertlshandshake":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/netprofile **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/netprofile? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/netprofile? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of netprofile resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/netprofile? **view=summary**

Use this query-parameter to get the summary output of netprofile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/netprofile? **pagesize=#no;pageno=#no**

Use this query-parameter to get the netprofile resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "netprofile": [ {

"name":<String_value>,

"srcip":<String_value>,

"td":<Integer_value>,

"srcippersistency":<String_value>,

"overridelsn":<String_value>,

"mbf":<String_value>,

"proxyprotocol":<String_value>,

"proxyprotocoltxversion":<String_value>,

"proxyprotocolaftertlshandshake":<String_value>,

"proxyprotocoltlvoptions":<String[]_value>,

"badipactionthreshold":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/netprofile/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/netprofile/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/netprofile/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of netprofile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "netprofile": [ {

"name":<String_value>,

"srcip":<String_value>,

"td":<Integer_value>,
```

```
"srcippersistency":<String_value>,

"overridelsn":<String_value>,

"mbf":<String_value>,

"proxyprotocol":<String_value>,

"proxyprotocoltxversion":<String_value>,

"proxyprotocolaftertlshandshake":<String_value>,

"proxyprotocoltlvoptions":<String[]_value>,

"badipactionthreshold":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/netprofile? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "netprofile": [ { "__count": "#no"} ] }
```

netprofile_binding

Binding object which returns the resources bound to netprofile.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the net profile whose details you want to display. Minimum length = 1
netprofile_natrule_binding	<netprofile_natrule_binding[]>	Read-only	natrule that can be bound to netprofile.
netprofile_srcportset_binding	<netprofile_srcportset_binding[]>	Read-only	srcportset that can be bound to netprofile.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/netprofile_binding/ name_value<String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "netprofile_binding": [ {

"name":<String_value>,

"netprofile_natrule_binding":<netprofile_natrule_binding[]_value>,
```

```
"netprofile_srcportset_binding":<netprofile_srcportset_binding[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/netprofile_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/netprofile_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "netprofile_binding": [ {

"name":<String_value>,

"netprofile_natrule_binding":<netprofile_natrule_binding[]_value>,

"netprofile_srcportset_binding":<netprofile_srcportset_binding[]_value>

}]}
```

netprofile_natrule_binding

Binding object showing the natrule that can be bound to netprofile.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
netmask	<String>	Read-write	.
natrule	<String>	Read-write	IPv4 network address on whose traffic you want the Citrix ADC to do rewrite ip prefix.
name	<String>	Read-write	Name of the netprofile to which to bind port ranges. Minimum length = 1
rewriteip	<String>	Read-write	.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/netprofile_natrule_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"netprofile_natrule_binding":{

<b>"name":<String_value>,

</b>"natrule":<String_value>,

"netmask":<String_value>,

"rewriteip":<String_value>
```

```
}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/netprofile_natrule_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ netprofile_natrule_binding/ name_value<String> ? **args=natrule: <String_value> ,netmask: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/netprofile_natrule_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ netprofile_natrule_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of netprofile_natrule_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/netprofile_natrule_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the netprofile_natrule_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "netprofile_natrule_binding": [ {

"netmask":<String_value>,

"natrule":<String_value>,

"name":<String_value>,

"rewriteip":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/netprofile_natrule_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/netprofile_natrule_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "netprofile_natrule_binding": [ {

"netmask":<String_value>,

"natrule":<String_value>,

"name":<String_value>,

"rewriteip":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/netprofile_natrule_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"netprofile_natrule_binding": [ { "__count": "#no"} ] }
```

netprofile_srcportset_binding

Binding object showing the srcportset that can be bound to netprofile.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the netprofile to which to bind port ranges. Minimum length = 1
srcportrange	<String>	Read-write	When the source port range is configured and associated with the netprofile bound to a service group, Citrix ADC will choose a port from the range configured for connection establishment at the backend servers. Minimum length = 1024 Maximum length = 65535
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD

- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/netprofile_srcportset_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"netprofile_srcportset_binding":{

<b>"name":<String_value>,

</b>"srcportrange":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/netprofile_srcportset_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ netprofile_srcportset_binding/ name_value<String> ? **args=srcportrange: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/netprofile_srcportset_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ netprofile_srcportset_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of netprofile_srcportset_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/netprofile_srcportset_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the netprofile_srcportset_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "netprofile_srcportset_binding": [ {

"name":<String_value>,

"srcportrange":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/netprofile_srcportset_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ netprofile_srcportset_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "netprofile_srcportset_binding": [ {

"name":<String_value>,

"srcportrange":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/netprofile_srcportset_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"netprofile_srcportset_binding": [ { "__count": "#no"} ] }
```

onlinkipv6prefix

Configuration for on-link IPv6 global prefixes for Router Advertisment resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ipv6prefix	<String>	Read-write	Onlink prefixes for RA messages.
onlinkprefix	<String>	Read-write	RA Prefix onlink flag. Default value: YES Possible values = YES, NO
autonomusprefix	<String>	Read-write	RA Prefix Autonomus flag. Default value: YES Possible values = YES, NO
depricateprefix	<String>	Read-write	Depricate the prefix. Default value: NO Possible values = YES, NO
decrementprefixlifetimes	<String>	Read-write	RA Prefix Autonomus flag. Default value: NO

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = YES, NO
prefixvalidelifetime	<Integer>	Read-write	Valide life time of the prefix, in seconds. Default value: 2592000
prefixpreferredlifetime	<Integer>	Read-write	Preferred life time of the prefix, in seconds. Default value: 604800
prefixcurrvalidelft	<Integer>	Read-only	Prefix current valid life time.
prefixcurrpreferredlft	<Integer>	Read-only	Prefix current prefered life time.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/onlinkipv6prefix **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"onlinkipv6prefix":{

<b>"ipv6prefix":<String_value>,

</b>"onlinkprefix":<String_value>,

"autonomusprefix":<String_value>,
```

```
"depricateprefix":<String_value>,

"decrementprefixlifetimes":<String_value>,

"prefixvalidelifetime":<Integer_value>,

"prefixpreferredlifetime":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/onlinkipv6prefix/ ipv6prefix_value<String>
HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/onlinkipv6prefix **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"onlinkipv6prefix":{

<b>"ipv6prefix":<String_value>,
```

```
</b>"onlinkprefix":<String_value>,

"autonomusprefix":<String_value>,

"depricateprefix":<String_value>,

"decrementprefixlifetimes":<String_value>,

"prefixvalidelifetime":<Integer_value>,

"prefixpreferredlifetime":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/onlinkipv6prefix? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"onlinkipv6prefix":{

<b>"ipv6prefix":<String_value>,

</b>"onlinkprefix":true,

"autonomusprefix":true,

"depricateprefix":true,
```

```
"decrementprefixlifetimes":true,

"prefixvalidelifetime":true,

"prefixpreferredlifetime":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/onlinkipv6prefix **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/onlinkipv6prefix? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/onlinkipv6prefix? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of onlinkipv6prefix resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/onlinkipv6prefix? **view=summary**

Use this query-parameter to get the summary output of onlinkipv6prefix resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/onlinkipv6prefix? **pagesize=#no;pageno=#no**

Use this query-parameter to get the onlinkipv6prefix resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "onlinkipv6prefix": [ {

"ipv6prefix":<String_value>,

"onlinkprefix":<String_value>,

"autonomusprefix":<String_value>,

"depricateprefix":<String_value>,

"decrementprefixlifetimes":<String_value>,

"prefixvalidelifetime":<Integer_value>,

"prefixpreferredlifetime":<Integer_value>,

"prefixcurrvalidelft":<Integer_value>,

"prefixcurrpreferredlft":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/onlinkipv6prefix/ ipv6prefix_value<String>
Query-parameters: attrs http:// <netscaler-ip-address> /nitro/v1/config/onlinkipv6prefix/ ipv6prefix_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/onlinkipv6prefix/ ipv6prefix_value<String> ? **view=summary**

Use this query-parameter to get the summary output of onlinkipv6prefix resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "onlinkipv6prefix": [ {

"ipv6prefix":<String_value>,

"onlinkprefix":<String_value>,

"autonomusprefix":<String_value>,

"depricateprefix":<String_value>,
```

```
"decrementprefixlifetimes":<String_value>,

"prefixvalidelifetime":<Integer_value>,

"prefixpreferredlifetime":<Integer_value>,

"prefixcurrvalidelft":<Integer_value>,

"prefixcurrpreferredlft":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/onlinkipv6prefix? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "onlinkipv6prefix": [ { "__count": "#no"} ] }
```

portallocation

Configuration for portallocation resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
srcip	<String>	Read-write	IP address for which Port allocation needs to be seen. IP address can be SNIP/VIP/NSIP.
destip	<String>	Read-write	Destination IP address or Server IP for which Port allocation needs to be seen.
destport	<Integer>	Read-write	Destination Port or Server port configuration. Minimum value = 1 Maximum value = 65535
protocol	<Integer>	Read-write	Protocol for the traffic. TCP traffic: 1, All other protocol traffic: 0. Minimum value = 0 Maximum value = 1
nodeid	<Integer>	Read-write	Unique number that identifies the cluster node. Minimum value = 0 Maximum value = 31

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
freeports	<Integer>	Read-only	Freeports for the desired IP address and other parameters. Minimum value = 0 Maximum value = 2147483647
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/portallocation **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/portallocation? **args=srcip: <String_value> , destip:<String_value>, destport:<Integer_value>, protocol:<Integer_value>, nodeid: <Integer_value>**

Use this query-parameter to get portallocation resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/config/portallocation? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/portallocation? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of portallocation resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/portallocation? **view=summary**

Use this query-parameter to get the summary output of portallocation resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/portallocation? **pagesize=#no;pageno=#no**

Use this query-parameter to get the portallocation resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "portallocation": [ {

srcip:<String_value>,<b>destip:<String_value>,</
b><b>destport:<Integer_value>,</b><b>protocol:<Integer_value>,</
b>nodeid:<Integer_value>"freeports":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/portallocation? **args=srcip: <String_value> , destip:<String_value>, destport:<Integer_value>, protocol:<Integer_value>, nodeid: <Integer_value> ;count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "portallocation": [ { "__count": "#no"} ] }
```

ptp

Configuration for Precision Time Protocol resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
state	<String>	Read-write	Enables or disables Precision Time Protocol (PTP) on the appliance. If you disable PTP, make sure you enable Network Time Protocol (NTP) on the cluster. Default value: ENABLE Possible values = DISABLE, ENABLE
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- UPDATE
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/ptp **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"ptp":{

<b>"state":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/ptp **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "ptp": [ {

"state":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

rnat

Configuration for RNAT configured route resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
network	<String>	Read-write	The network address defined for the RNAT entry. Minimum length = 1
netmask	<String>	Read-write	The subnet mask for the network address. Minimum length = 1
aclname	<String>	Read-write	An extended ACL defined for the RNAT entry. Minimum length = 1
td	<Integer>	Read-write	Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0. Minimum value = 0 Maximum value = 4094
ownergroup	<String>	Read-write	The owner node group in a Cluster for this rnat rule. Default value: DEFAULT_NG Minimum length = 1
name	<String>	Read-write	Name for the RNAT4 rule. Must begin with a letter, number, or

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			the underscore character (_), and can consist of letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore characters. Cannot be changed after the rule is created. Choose a name that helps identify the RNAT4 rule. Minimum length = 1
redirectport	<Integer>	Read-write	Port number to which the IPv4 packets are redirected. Applicable to TCP and UDP protocols. Minimum value = 1 Maximum value = 65535
natip	<String>	Read-write	Any NetScaler-owned IPv4 address except the NSIP address. The NetScaler appliance replaces the source IP addresses of server-generated packets with the IP address specified. The IP address must be a public NetScaler-owned IP address. If you

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			specify multiple addresses for this field, NATIP selection uses the round robin algorithm for each session. By specifying a range of IP addresses, you can specify all NetScaler-owned IP addresses, except the NSIP, that fall within the specified range. Minimum length = 1
srcippersistency	<String>	Read-write	Enables the Citrix ADC to use the same NAT IP address for all RNAT sessions initiated from a particular server. Default value: DISABLED Possible values = ENABLED, DISABLED
useproxyport	<String>	Read-write	Enable source port proxying, which enables the Citrix ADC to use the RNAT ips using proxied source port. Default value: ENABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ENABLED, DISABLED
connfailover	<String>	Read-write	Synchronize all connection-related information for the RNAT sessions with the secondary ADC in a high availability (HA) pair. Default value: DISABLED Possible values = ENABLED, DISABLED
newname	<String>	Read-write	New name for the RNAT4 rule. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Minimum length = 1
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- CLEAR
- UPDATE
- UNSET
- ADD
- RENAME
- DELETE
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

CLEAR

URL: http:// <netscaler-ip-address> /nitro/v1/config/rnat? **action=clear HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"rnat":{

"network":<String_value>,

"netmask":<String_value>,

"aclname":<String_value>,

"td":<Integer_value>,

"ownergroup":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/rnat **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"rnat":{

"name":<String_value>,

"network":<String_value>,
```

```
"netmask":<String_value>,

"aclname":<String_value>,

"redirectport":<Integer_value>,

"td":<Integer_value>,

"natip":<String_value>,

"srcippersistency":<String_value>,

"useproxyport":<String_value>,

"ownergroup":<String_value>,

"connfailover":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/rnat? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"rnat":{

"name":<String_value>,

"network":true,
```

```
"netmask":true,

"aclname":true,

"td":true,

"redirectport":true,

"natip":true,

"srcippersistency":true,

"ownergroup":true,

"useproxyport":true,

"connfailover":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/rnat **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"rnat":{

<b>"name":<String_value>,

</b>"network":<String_value>,
```

```
"netmask":<String_value>,

"aclname":<String_value>,

"redirectport":<Integer_value>,

"td":<Integer_value>,

"srcippersistency":<String_value>,

"useproxyport":<String_value>,

"connfailover":<String_value>,

"ownergroup":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

RENAME

URL: http:// <netscaler-ip-address> /nitro/v1/config/rnat? **action=rename HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"rnat":{

<b>"name":<String_value>,

</b><b>"newname":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/rnat/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/rnat **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/rnat? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/rnat? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of rnat resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/rnat? **view=summary**

Use this query-parameter to get the summary output of rnat resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/rnat? **pagesize=#no;pageno=#no**

Use this query-parameter to get the rnat resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "rnat": [ {

"name":<String_value>,

"network":<String_value>,

"netmask":<String_value>,

"td":<Integer_value>,

"natip":<String_value>,

"aclname":<String_value>,

"redirectport":<Integer_value>,

"srcippersistency":<String_value>,

"useproxyport":<String_value>,

"ownergroup":<String_value>,

"connfailover":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/rnat/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/rnat/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/rnat/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of rnat resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "rnat": [ {

"name":<String_value>,

"network":<String_value>,

"netmask":<String_value>,

"td":<Integer_value>,

"natip":<String_value>,

"aclname":<String_value>,
```

```
"redirectport":<Integer_value>,

"srcippersistency":<String_value>,

"useproxyport":<String_value>,

"ownergroup":<String_value>,

"connfailover":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/rnat? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "rnat": [ { "__count": "#no"} ] }
```

rnat6

Configuration for IPv6 RNAT configured route resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the RNAT6 rule. Must begin with a letter, number, or the underscore character (_), and can consist of letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore characters. Cannot be changed after the rule is created. Choose a name that helps identify the RNAT6 rule. Minimum length = 1
network	<String>	Read-write	IPv6 address of the network on whose traffic you want the Citrix ADC to do RNAT processing. Minimum length = 1
acl6name	<String>	Read-write	Name of any configured ACL6 whose action is ALLOW. The rule of the ACL6 is used as an RNAT6 rule. Minimum length = 1
redirectport	<Integer>	Read-write	Port number to which the IPv6 packets are

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			redirected. Applicable to TCP and UDP protocols. Minimum value = 1 Maximum value = 65535
td	<Integer>	Read-write	Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0. Minimum value = 0 Maximum value = 4094
srcippersistency	<String>	Read-write	Enable source ip persistency, which enables the Citrix ADC to use the RNAT ips using source ip. Default value: DISABLED Possible values = ENABLED, DISABLED
ownergroup	<String>	Read-write	The owner node group in a Cluster for this rnat rule.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: DEFAULT_NG Minimum length = 1
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- UPDATE
- UNSET
- CLEAR
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/rnat6 **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"rnat6":{

<b>"name":<String_value>,

</b>"network":<String_value>,

"acl6name":<String_value>,

"redirectport":<Integer_value>,

"td":<Integer_value>,

"srcippersistency":<String_value>,

"ownergroup":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/rnat6 **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"rnat6":{

<b>"name":<String_value>,

</b>"redirectport":<Integer_value>,

"srcippersistency":<String_value>,

"ownergroup":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/rnat6? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"rnat6":{

<b>"name":<String_value>,
```

```
</b>"redirectport":true,

"srcippersistency":true,

"ownergroup":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

CLEAR

URL: http:// <netscaler-ip-address> /nitro/v1/config/rnat6? **action=clear HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"rnat6":{

<b>"name":<String_value>,

</b>"ownergroup":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/rnat6 **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/rnat6? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/rnat6? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of rnat6 resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/rnat6? **view=summary**

Use this query-parameter to get the summary output of rnat6 resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/rnat6? **pagesize=#no;pageno=#no**

Use this query-parameter to get the rnat6 resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "rnat6": [ {

"name":<String_value>,

"network":<String_value>,

"td":<Integer_value>,
```

```
"acl6name":<String_value>,

"redirectport":<Integer_value>,

"srcippersistency":<String_value>,

"ownergroup":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/rnat6/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/rnat6/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/rnat6/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of rnat6 resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "rnat6": [ {

"name":<String_value>,

"network":<String_value>,

"td":<Integer_value>,

"acl6name":<String_value>,

"redirectport":<Integer_value>,

"srcippersistency":<String_value>,

"ownergroup":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/rnat6? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "rnat6": [ { "__count": "#no"} ] }
```

rnat6_binding

Binding object which returns the resources bound to rnat6.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the RNAT6 rule whose details you want to display. Minimum length = 1
rnat6_nsip6_binding	<rnat6_nsip6_binding[]>	Read-only	nsip6 that can be bound to rnat6.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/rnat6_binding/ name_value<String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "rnat6_binding": [ {

"name":<String_value>,

"rnat6_nsip6_binding":<rnat6_nsip6_binding[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/rnat6_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/rnat6_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "rnat6_binding": [ {

"name":<String_value>,

"rnat6_nsip6_binding":<rnat6_nsip6_binding[]_value>

}]}
```

rnat6_nsip6_binding

Binding object showing the nsip6 that can be bound to rnat6.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
natip6	<String>	Read-write	Nat IP Address. Minimum length = 1
ownergroup	<String>	Read-write	The owner node group in a Cluster for this rnat rule. Default value: DEFAULT_NG Minimum length = 1
name	<String>	Read-write	Name of the RNAT6 rule to which to bind NAT IPs. Minimum length = 1
td	<Integer>	Read-only	Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0. Minimum value = 0 Maximum value = 4094
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/rnat6_nsip6_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"rnat6_nsip6_binding":{

<b>"name":<String_value>,

</b><b>"natip6":<String_value>,

</b>"ownergroup":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/rnat6_nsip6_binding/ name_value<String>
Query-parameters: args http:// <netscaler-ip-address> /nitro/v1/config/rnat6_nsip6_binding/ name_value<String> ? **args= natip6:<String_value>, ownergroup: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/rnat6_nsip6_binding/ name_value<String>
Query-parameters: filter http:// <netscaler-ip-address> /nitro/v1/config/rnat6_nsip6_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of rnat6_nsip6_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/rnat6_nsip6_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the rnat6_nsip6_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "rnat6_nsip6_binding": [ {

"natip6":<String_value>,

"ownergroup":<String_value>,

"name":<String_value>,

"td":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/rnat6_nsip6_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ rnat6_nsip6_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "rnat6_nsip6_binding": [ {

"natip6":<String_value>,

"ownergroup":<String_value>,

"name":<String_value>,

"td":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/rnat6_nsip6_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"rnat6_nsip6_binding": [ { "__count": "#no"} ] }
```

rnat_binding

Binding object which returns the resources bound to rnat.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the RNAT rule whose details you want to display. Minimum length = 1
rnat_retainsourceportset_binding	<rnat_retainsourceportset_binding[]>	Read-only	retainsourceportset that can be bound to rnat.
rnat_nsip_binding	<rnat_nsip_binding[]>	Read-only	nsip that can be bound to rnat.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/rnat_binding/ name_value<String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "rnat_binding": [ {

"name":<String_value>,

"rnat_nsip_binding":<rnat_nsip_binding[]_value>,

"rnat_retainsourceportset_binding":<rnat_retainsourceportset_binding[]_val
ue>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/rnat_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/rnat_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "rnat_binding": [ {

"name":<String_value>,

"rnat_nsip_binding":<rnat_nsip_binding[]_value>,

"rnat_retainsourceportset_binding":<rnat_retainsourceportset_binding[]_val
ue>

}]}
```

rnat_nsip_binding

Binding object showing the nsip that can be bound to rnat.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
natip	<String>	Read-write	Any NetScaler-owned IPv4 address except the NSIP address. The NetScaler appliance replaces the source IP addresses of server-generated packets with the IP address specified. The IP address must be a public NetScaler-owned IP address. If you specify multiple addresses for this field, NATIP selection uses the round robin algorithm for each session. By specifying a range of

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			IP addresses, you can specify all NetScaler-owned IP addresses, except the NSIP, that fall within the specified range. Minimum length = 1
name	<String>	Read-write	Name of the RNAT rule to which to bind NAT IPs. Minimum length = 1
td	<Integer>	Read-only	Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0. Minimum value = 0 Maximum value = 4094
ownergroup	<String>	Read-only	The owner node group in a Cluster for this rnat rule. Default value: DEFAULT_NG Minimum length = 1
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/rnat_nsip_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"rnat_nsip_binding":{

<b>"name":<String_value>,

</b>"natip":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/rnat_nsip_binding/ name_value<String>
Query-parameters: args http:// <netscaler-ip-address> /nitro/v1/config/rnat_nsip_binding/ name_value<String> ? **args=natip: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/rnat_nsip_binding/ name_value<String>
Query-parameters: filter http:// <netscaler-ip-address> /nitro/v1/config/rnat_nsip_binding/

name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of rnat_nsip_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/rnat_nsip_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the rnat_nsip_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "rnat_nsip_binding": [ {

"natip":<String_value>,

"name":<String_value>,

"td":<Integer_value>,

"ownergroup":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/rnat_nsip_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ rnat_nsip_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "rnat_nsip_binding": [ {

"natip":<String_value>,

"name":<String_value>,

"td":<Integer_value>,

"ownergroup":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/rnat_nsip_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"rnat_nsip_binding": [ { "__count": "#no"} ] }
```

rnat_retainsourceportset_binding

Binding object showing the retainsourceportset that can be bound to rnat.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
retainsourceportrange	<String>	Read-write	When the source port range is configured and associated with the RNAT rule, Citrix ADC will choose a port from the specified source port range configured for connection establishment at the backend servers.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum length = 1024 Maximum length = 65535
name	<String>	Read-write	Name of the RNAT rule to which to bind NAT IPs. Minimum length = 1
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.
- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/rnat_retainsourceportset_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"rnat_retainsourceportset_binding":{

<b>"name":<String_value>,

</b>"retainsourceportrange":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/rnat_retainsourceportset_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ rnat_retainsourceportset_binding/ name_value<String> ? **args=retainsourceportrange: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/rnat_retainsourceportset_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ rnat_retainsourceportset_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of rnat_retainsourceportset_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/rnat_retainsourceportset_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the rnat_retainsourceportset_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "rnat_retainsourceportset_binding": [ {

"retainsourceportrange":<String_value>,

"name":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/rnat_retainsourceportset_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/rnat_retainsourceportset_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "rnat_retainsourceportset_binding": [ {

"retainsourceportrange":<String_value>,

"name":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/rnat_retainsourceportset_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"rnat_retainsourceportset_binding": [ { "__count": "#no"} ] }
```

rnatglobal_auditsyslogpolicy_binding

Binding object showing the auditsyslogpolicy that can be bound to rnatglobal.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
policy	<String>	Read-write	The policy Name.
all	<Boolean>	Read-write	Remove all RNAT global config.
priority	<Integer>	Read-write	The priority of the policy.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- GET
- COUNT
- ADD
- DELETE

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/rnatglobal_auditsyslogpolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"rnatglobal_auditsyslogpolicy_binding":{

"policy":<String_value>,

"priority":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/rnatglobal_auditsyslogpolicy_binding **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/rnatglobal_auditsyslogpolicy_binding? **args=policy: <String_value> ,all: <Boolean_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/rnatglobal_auditsyslogpolicy_binding **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/rnatglobal_auditsyslogpolicy_binding? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of rnatglobal_auditsyslogpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/rnatglobal_auditsyslogpolicy_binding? **pagesize=#no;pageno=#no**

Use this query-parameter to get the rnatglobal_auditsyslogpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "rnatglobal_auditsyslogpolicy_binding": [ {

"policy":<String_value>,

"all":<Boolean_value>,
```

```
"priority":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/rnatglobal_auditsyslogpolicy_binding?**count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "rnatglobal_auditsyslogpolicy_binding": [ { "__count": "#no"} ] }
```

rnatglobal_binding

Binding object which returns the resources bound to rnatglobal.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
rnatglobal_auditsyslogpolicy_binding	<rnatglobal_auditsyslogpolicy_binding[]>	Read-write	auditsyslogpolicy that can be bound to rnatglobal.

Operations

(click to see Properties)

- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/rnatglobal_binding

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "rnatglobal_binding": [ {

"rnatglobal_auditsyslogpolicy_binding":<rnatglobal_auditsyslogpolicy_binding[]_value>

}]}
```

rnatparam

Configuration for RNAT parameter resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
tcpproxy	<String>	Read-write	Enable TCP proxy, which enables the Citrix ADC to optimize the RNAT TCP traffic by using Layer 4 features. Default value: ENABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ENABLED, DISABLED
srcippersistency	<String>	Read-write	Enable source ip persistency, which enables the Citrix ADC to use the RNAT ips using source ip. Default value: DISABLED Possible values = ENABLED, DISABLED
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- UPDATE
- UNSET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.
- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of

creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/rnatparam **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"rnatparam":{

"tcpproxy":<String_value>,

"srcippersistency":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/rnatparam? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"rnatparam":{

"tcpproxy":true,

"srcippersistency":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/rnatparam **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "rnatparam": [ {

"tcpproxy":<String_value>,

"srcippersistency":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

rnatsession

Configuration for RNAT session resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
network	<String>	Read-write	IPv4 network address on whose traffic you want the Citrix ADC to do RNAT processing. Minimum length = 1
netmask	<String>	Read-write	Subnet mask associated with the network address. Minimum length = 1
natip	<String>	Read-write	The NAT IP address defined for the RNAT entry. Minimum length = 1
aclname	<String>	Read-write	Name of any configured extended ACL whose action is ALLOW.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum length = 1

Operations

(click to see Properties)

- FLUSH

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

FLUSH

URL: http:// <netscaler-ip-address> /nitro/v1/config/rnatsession? **action=flush HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"rnatsession":{

"network":<String_value>,

"netmask":<String_value>,

"natip":<String_value>,

"aclname":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

route

Configuration for route resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
network	<String>	Read-write	IPv4 network address for which to add a route entry in the routing table of the Citrix ADC.
netmask	<String>	Read-write	The subnet mask associated with the network address.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
gateway	<String>	Read-write	IP address of the gateway for this route. Can be either the IP address of the gateway, or can be null to specify a null interface route. Minimum length = 1
vlan	<Integer>	Read-write	VLAN as the gateway for this route. Minimum value = 1 Maximum value = 4094
cost	<Integer>	Read-write	Positive integer used by the routing algorithms to determine preference for using this route. The lower the cost, the higher the preference. Minimum value = 0 Maximum value = 65535
td	<Integer>	Read-write	Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			domain, which has an ID of 0. Minimum value = 0 Maximum value = 4094
distance	<Integer>	Read-write	Administrative distance of this route, which determines the preference of this route over other routes, with same destination, from different routing protocols. A lower value is preferred. Default value: 1 Minimum value = 0 Maximum value = 255
cost1	<Integer>	Read-write	The cost of a route is used to compare routes of the same type. The route having the lowest cost is the most preferred route. Possible values: 0 through 65535. Default: 0. Minimum value = 0 Maximum value = 65535

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
weight	<Integer>	Read-write	Positive integer used by the routing algorithms to determine preference for this route over others of equal cost. The lower the weight, the higher the preference. Default value: 1 Minimum value = 1 Maximum value = 65535
advertise	<String>	Read-write	Advertise this route. Possible values = DISABLED, ENABLED
protocol	<String[]>	Read-write	Routing protocol used for advertising this route. Default value: ADV_ROUTE_FLAGS Possible values = OSPF, ISIS, RIP, BGP
msr	<String>	Read-write	Monitor this route using a monitor of type ARP or PING. Default value: DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ENABLED, DISABLED
monitor	<String>	Read-write	Name of the monitor, of type ARP or PING, configured on the Citrix ADC to monitor this route. Minimum length = 1
ownergroup	<String>	Read-write	The owner node group in a Cluster for this route. If owner node group is not specified then the route is treated as Striped route. Default value: DEFAULT_NG Minimum length = 1
mgmt	<Boolean>	Read-write	Route in management plane.
routetype	<String>	Read-write	Protocol used by routes that you want to remove from the routing table of the Citrix ADC. Possible values = CONNECTED, STATIC, DYNAMIC, OSPF, ISIS, RIP, BGP
detail	<Boolean>	Read-write	Display a detailed view.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
gatewayname	<String>	Read-only	The name of the gateway for this route. For a route other than a link load balancing (LLB) route, this value is null.
type	<Boolean>	Read-only	State of the RNAT.
dynamic	<Boolean>	Read-only	State of the route.
Static	<Boolean>	Read-only	.
permanent	<Boolean>	Read-only	.
direct	<Boolean>	Read-only	.
nat	<Boolean>	Read-only	.
lbroute	<Boolean>	Read-only	.
adv	<Boolean>	Read-only	.
tunnel	<Boolean>	Read-only	Show whether it is a tunnel route or not.
data	<Boolean>	Read-only	Internal data of this route.
data0	<Boolean>	Read-only	Internal route type is stored, used for get.
flags	<Boolean>	Read-only	If this route is dynamic, the name of the routing protocol from which it was learned.
routeowners	<String[]>	Read-only	Use this option with -dynamic and in a cluster only to

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			specify the set of nodes from which this dynamic route has been learnt. Possible values = 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31
retain	<Integer>	Read-only	.
ospf	<Boolean>	Read-only	OSPF protocol.
isis	<Boolean>	Read-only	ISIS protocol.
rip	<Boolean>	Read-only	RIP protocol.
bgp	<Boolean>	Read-only	BGP protocol.
dhcp	<Boolean>	Read-only	.
advospf	<Boolean>	Read-only	Advertised through OSPF protocol.
advisis	<Boolean>	Read-only	Advertised through ISIS protocol.
advrip	<Boolean>	Read-only	Advertised through RIP protocol.
advbgp	<Boolean>	Read-only	Advertised through BGP protocol.
state	<Integer>	Read-only	The state of the static route. Possible values: UP, DOWN.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
totalprobes	<Integer>	Read-only	The total number of probes sent.
totalfailedprobes	<Integer>	Read-only	The total number of failed probes.
failedprobes	<Integer>	Read-only	Number of the current failed monitoring probes.
monstatcode	<Integer>	Read-only	The code indicating the monitor response.
monstatparam1	<Integer>	Read-only	First parameter used with the message code.
monstatparam2	<Integer>	Read-only	Second parameter used with the message code.
monstatparam3	<Integer>	Read-only	Third parameter used with the message code.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- CLEAR
- DELETE
- UPDATE
- UNSET
- GET (ALL)

- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/route **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"route":{

<b>"network":<String_value>,
```

```
</b><b>"netmask":<String_value>,

</b>"gateway":<String_value>,

"vlan":<Integer_value>,

"cost":<Integer_value>,

"td":<Integer_value>,

"distance":<Integer_value>,

"cost1":<Integer_value>,

"weight":<Integer_value>,

"advertise":<String_value>,

"protocol":<String[]_value>,

"msr":<String_value>,

"monitor":<String_value>,

"ownergroup":<String_value>,

"mgmt":<Boolean_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

CLEAR

URL: http:// <netscaler-ip-address> /nitro/v1/config/route? **action=clear HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"route":{

<b>"routetype":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/route/ network_value<String> **Query-parameters: args= netmask:<String_value>, gateway: <String_value> ,vlan: <Integer_value> ,td: <Integer_value> ,ownergroup: <String_value> ,mgmt: <Boolean_value>**
update
URL: http:// <netscaler-ip-address> /nitro/v1/config/route **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"route":{

<b>"network":<String_value>,

</b><b>"netmask":<String_value>,

</b><b>"gateway":<String_value>,

</b>"td":<Integer_value>,

"distance":<Integer_value>,
```

```
"cost1":<Integer_value>,

"weight":<Integer_value>,

"advertise":<String_value>,

"protocol":<String[]_value>,

"msr":<String_value>,

"monitor":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

unset

URL: http:// <netscaler-ip-address> /nitro/v1/config/route? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"route":{

<b>"network":<String_value>,

</b><b>"netmask":<String_value>,

</b><b>"gateway":<String_value>,

</b>"td":<Integer_value>,

"advertise":true,
```

```
"distance":true,

"cost1":true,

"weight":true,

"protocol":true,

"msr":true,

"monitor":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error
get (all)
URL: http:// <netscaler-ip-address> /nitro/v1/config/route **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/route? **args=network: <String_value> ,netmask: <String_value> ,gateway: <String_value> ,vlan: <Integer_value> ,td: <Integer_value> ,routetype: <String_value> ,detail: <Boolean_value> ,mgmt: <Boolean_value>**

Use this query-parameter to get route resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/config/route? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/route? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of route resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/route? **view=summary**

Use this query-parameter to get the summary output of route resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/route? **pagesize=#no;pageno=#no**

Use this query-parameter to get the route resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "route": [ {

network:<String_value>,netmask:<String_value>,gateway:<String_value>,vlan:
<Integer_value>,td:<Integer_value>,routetype:<String_value>,detail:<Boolea
n_value>,mgmt:<Boolean_value>"gatewayname":<String_value>,

"advertise":<String_value>,

"type":<Boolean_value>,

"dynamic":<Boolean_value>,

"Static":<Boolean_value>,

"permanent":<Boolean_value>,

"direct":<Boolean_value>,

"nat":<Boolean_value>,
```

```
"lbroute":<Boolean_value>,

"adv":<Boolean_value>,

"tunnel":<Boolean_value>,

"cost":<Integer_value>,

"distance":<Integer_value>,

"cost1":<Integer_value>,

"weight":<Integer_value>,

"protocol":<String[]_value>,

"data":<Boolean_value>,

"data0":<Boolean_value>,

"flags":<Boolean_value>,

"routeowners":<String[]_value>,

"retain":<Integer_value>,

"ospf":<Boolean_value>,

"isis":<Boolean_value>,

"rip":<Boolean_value>,

"bgp":<Boolean_value>,

"dhcp":<Boolean_value>,

"advospf":<Boolean_value>,

"advisis":<Boolean_value>,

"advrip":<Boolean_value>,

"advbgp":<Boolean_value>,
```

```
"msr":<String_value>,

"monitor":<String_value>,

"state":<Integer_value>,

"totalprobes":<Integer_value>,

"totalfailedprobes":<Integer_value>,

"failedprobes":<Integer_value>,

"monstatcode":<Integer_value>,

"monstatparam1":<Integer_value>,

"monstatparam2":<Integer_value>,

"monstatparam3":<Integer_value>,

"ownergroup":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

count

URL: http:// <netscaler-ip-address> /nitro/v1/config/route? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "route": [ { "__count": "#no"} ] }
```

route6

Configuration for route 6 resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
network	<String>	Read-write	IPv6 network address for which to add a route entry to the routing table of the Citrix ADC.
gateway	<String>	Read-write	The gateway for this route. The value for this parameter is either an IPv6 address or null. Default value: 0
vlan	<Integer>	Read-write	Integer value that uniquely identifies a VLAN through which the Citrix ADC forwards the packets for this route. Default value: 0 Minimum value = 0 Maximum value = 4094

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
vxlan	<Integer>	Read-write	Integer value that uniquely identifies a VXLAN through which the Citrix ADC forwards the packets for this route. Minimum value = 1 Maximum value = 16777215
weight	<Integer>	Read-write	Positive integer used by the routing algorithms to determine preference for this route over others of equal cost. The lower the weight, the higher the preference. Default value: 1 Minimum value = 1 Maximum value = 65535
distance	<Integer>	Read-write	Administrative distance of this route from the appliance. Default value: 1 Minimum value = 1 Maximum value = 254
cost	<Integer>	Read-write	Positive integer used by the routing algorithms to

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			determine preference for this route. The lower the cost, the higher the preference. Default value: 1 Minimum value = 0 Maximum value = 65535
advertise	<String>	Read-write	Advertise this route. Possible values = DISABLED, ENABLED
msr	<String>	Read-write	Monitor this route with a monitor of type ND6 or PING. Default value: DISABLED Possible values = ENABLED, DISABLED
monitor	<String>	Read-write	Name of the monitor, of type ND6 or PING, configured on the Citrix ADC to monitor this route. Minimum length = 1
td	<Integer>	Read-write	Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			becomes part of the default traffic domain, which has an ID of 0. Minimum value = 0 Maximum value = 4094
ownergroup	<String>	Read-write	The owner node group in a Cluster for this route6. If owner node group is not specified then the route is treated as Striped route. Default value: DEFAULT_NG Minimum length = 1
mgmt	<Boolean>	Read-write	Route in management plane.
routetype	<String>	Read-write	Type of IPv6 routes to remove from the routing table of the Citrix ADC. Possible values = CONNECTED, STATIC, DYNAMIC, OSPF, ISIS, BGP, RIP, ND-RA-ROUTE, FIB6
detail	<Boolean>	Read-write	To get a detailed view.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
gatewayname	<String>	Read-only	The name of the gateway for this route.
type	<Boolean>	Read-only	State of the RNAT.
dynamic	<Boolean>	Read-only	Whether this route is dynamically learned or not.
data	<Boolean>	Read-only	Internal data of this route.
flags	<Boolean>	Read-only	For a dynamic route, the routing protocol from which the route was learned.
state	<Integer>	Read-only	Whether this route is UP or DOWN.
totalprobes	<Integer>	Read-only	The total number of probes sent.
totalfailedprobes	<Integer>	Read-only	The total number of failed probes.
failedprobes	<Integer>	Read-only	Current number of failed monitoring probes.
monstatcode	<Integer>	Read-only	The code indicating the monitor response.
monstatparam1	<Integer>	Read-only	First parameter for use with message code.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
monstatparam2	<Integer>	Read-only	Second parameter for use with message code.
monstatparam3	<Integer>	Read-only	Third parameter for use with message code.
data1	<String>	Read-only	Internal data of this route. Possible values = ENABLED, DISABLED
routeowners	<String[]>	Read-only	Use this option with -dynamic and in a cluster only to specify the set of nodes from which this dynamic route has been learnt. Possible values = 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31
retain	<Integer>	Read-only	.
Static	<Boolean>	Read-only	Static route.
permanent	<Boolean>	Read-only	Permanent Route.
connected	<Boolean>	Read-only	Connected Route.
ospfv3	<Boolean>	Read-only	For a dynamic route, the routing protocol

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			from which the route was learned.
isis	<Boolean>	Read-only	If this route is dynamic then which routing protocol was it learnt from.
active	<Boolean>	Read-only	For a dynamic route, the routing protocol from which the route was learned.
bgp	<Boolean>	Read-only	For a dynamic route, the routing protocol from which the route was learned.
rip	<Boolean>	Read-only	For a dynamic route, the routing protocol from which the route was learned.
raroute	<Boolean>	Read-only	For a dynamic route, the routing protocol from which the route was learned.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- CLEAR
- DELETE
- UPDATE

- UNSET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/route6 **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"route6":{

<b>"network":<String_value>,

</b>"gateway":<String_value>,

"vlan":<Integer_value>,

"vxlan":<Integer_value>,

"weight":<Integer_value>,

"distance":<Integer_value>,

"cost":<Integer_value>,

"advertise":<String_value>,

"msr":<String_value>,

"monitor":<String_value>,

"td":<Integer_value>,

"ownergroup":<String_value>,

"mgmt":<Boolean_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

CLEAR

URL: http:// <netscaler-ip-address> /nitro/v1/config/route6? **action=clear HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"route6":{

<b>"routetype":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/route6/ network_value<String> **Query-parameters: args=gateway: <String_value> ,vlan: <Integer_value> ,vxlan: <Integer_value> ,td: <Integer_value> ,ownergroup: <String_value> ,mgmt: <Boolean_value>**
update
URL: http:// <netscaler-ip-address> /nitro/v1/config/route6 **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"route6":{

<b>"network":<String_value>,

</b>"gateway":<String_value>,

"vlan":<Integer_value>,

"vxlan":<Integer_value>,

"weight":<Integer_value>,
```

```
"distance":<Integer_value>,

"cost":<Integer_value>,

"advertise":<String_value>,

"msr":<String_value>,

"monitor":<String_value>,

"td":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

unset

URL: http:// <netscaler-ip-address> /nitro/v1/config/route6? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"route6":{

<b>"network":<String_value>,

</b>"gateway":<String_value>,

"vlan":<Integer_value>,

"vxlan":<Integer_value>,

"td":<Integer_value>,
```

```
"weight":true,

"distance":true,

"cost":true,

"advertise":true,

"msr":true,

"monitor":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error
get (all)
URL: http:// <netscaler-ip-address> /nitro/v1/config/route6 **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/route6? **args=network: <String_value> ,gateway: <String_value> ,vlan: <Integer_value> ,vxlan: <Integer_value> ,td: <Integer_value> ,routetype: <String_value> ,detail: <Boolean_value> ,mgmt: <Boolean_value>**

Use this query-parameter to get route6 resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/config/route6? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/route6? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of route6 resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/route6? **view=summary**

Use this query-parameter to get the summary output of route6 resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/route6? **pagesize=#no;pageno=#no**

Use this query-parameter to get the route6 resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "route6": [ {

network:<String_value>,gateway:<String_value>,vlan:<Integer_value>,vxlan:<
Integer_value>,td:<Integer_value>,routetype:<String_value>,detail:<Boolean
_value>,mgmt:<Boolean_value>"gatewayname":<String_value>,

"advertise":<String_value>,

"type":<Boolean_value>,

"dynamic":<Boolean_value>,

"weight":<Integer_value>,

"distance":<Integer_value>,

"cost":<Integer_value>,

"data":<Boolean_value>,
```

```
"flags":<Boolean_value>,

"msr":<String_value>,

"monitor":<String_value>,

"state":<Integer_value>,

"totalprobes":<Integer_value>,

"totalfailedprobes":<Integer_value>,

"failedprobes":<Integer_value>,

"monstatcode":<Integer_value>,

"monstatparam1":<Integer_value>,

"monstatparam2":<Integer_value>,

"monstatparam3":<Integer_value>,

"data1":<String_value>,

"routeowners":<String[]_value>,

"retain":<Integer_value>,

"Static":<Boolean_value>,

"permanent":<Boolean_value>,

"connected":<Boolean_value>,

"ospfv3":<Boolean_value>,

"isis":<Boolean_value>,

"active":<Boolean_value>,

"bgp":<Boolean_value>,

"rip":<Boolean_value>,
```

```
"raroute":<Boolean_value>,

"ownergroup":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

count

URL: http:// <netscaler-ip-address> /nitro/v1/config/route6? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "route6": [ { "__count": "#no"} ] }
```

rsskeytype

Configuration for RSS key type resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
rsstype	<String>	Read-write	Type of RSS key, possible values are SYMMETRIC and ASYMMETRIC. Default value: ASYMMETRIC Possible values = ASYMMETRIC, SYMMETRIC
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- UPDATE
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/rsskeytype **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"rsskeytype":{

<b>"rsstype":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/rsskeytype **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "rsskeytype": [ {

"rsstype":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

vlan

Configuration for "VLAN" resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
id	<Integer>	Read-write	A positive integer that uniquely identifies a VLAN. Minimum value = 1 Maximum value = 4094
aliasname	<String>	Read-write	A name for the VLAN. Must begin with a letter, a number, or the underscore symbol, and can consist of from 1 to 31 letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			(=), colon (:), and underscore (_) characters. You should choose a name that helps identify the VLAN. However, you cannot perform any VLAN operation by specifying this name instead of the VLAN ID. Maximum length = 31
dynamicrouting	<String>	Read-write	Enable dynamic routing on this VLAN. Default value: DISABLED Possible values = ENABLED, DISABLED
ipv6dynamicrouting	<String>	Read-write	Enable all IPv6 dynamic routing protocols on this VLAN. Note: For the ENABLED setting to work, you must configure IPv6 dynamic routing protocols from the VTYSH command line. Default value: DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ENABLED, DISABLED
mtu	<Integer>	Read-write	Specifies the maximum transmission unit (MTU), in bytes. The MTU is the largest packet size, excluding 14 bytes of ethernet header and 4 bytes of crc, that can be transmitted and received over this VLAN. Default value: 0 Minimum value = 500 Maximum value = 9216
sharing	<String>	Read-write	If sharing is enabled, then this vlan can be shared across multiple partitions by binding it to all those partitions. If sharing is disabled, then this vlan can be bound to only one of the partitions. Default value: DISABLED Possible values = ENABLED, DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
linklocalipv6addr	<String>	Read-only	The link-local IP address assigned to the VLAN.
rnat	<Boolean>	Read-only	Temporary flag used for internal purpose.
portbitmap	<Integer>	Read-only	Member interfaces of this vlan.
lsbitmap	<Integer>	Read-only	Member linksets of this vlan.
tagbitmap	<Integer>	Read-only	Tagged members of this vlan.
lstagbitmap	<Integer>	Read-only	Tagged linksets of this vlan.
ifaces	<String>	Read-only	Names of all member interfaces of this vlan.
tagifaces	<String>	Read-only	Names of all tagged member interfaces of this vlan.
ifnum	<String>	Read-only	The interface to be bound to the VLAN, specified in slot/port notation (for example, 1/3). Minimum length = 1
tagged	<Boolean>	Read-only	Make the interface an 802.1q tagged interface. Packets sent on this interface on this VLAN have an additional 4-byte 802.1q tag, which

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			identifies the VLAN. To use 802.1q tagging, you must also configure the switch connected to the appliance's interfaces.
vlantd	<Integer>	Read-only	Traffic domain associated with vlan. Minimum value = 0 Maximum value = 4094
sdxvlan	<String>	Read-only	SDX vlan. Default value: NO Possible values = YES, NO
partitionname	<String>	Read-only	Name of the Partition to which this vlan bound to. Minimum length = 1
vxlan	<Integer>	Read-only	The VXLAN that extends this vlan.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE

- UNSET
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/vlan **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"vlan":{

<b>"id":<Integer_value>,

</b>"aliasname":<String_value>,

"dynamicrouting":<String_value>,

"ipv6dynamicrouting":<String_value>,

"mtu":<Integer_value>,

"sharing":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vlan/ id_value<Integer> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vlan **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"vlan":{

<b>"id":<Integer_value>,

</b>"aliasname":<String_value>,

"dynamicrouting":<String_value>,

"ipv6dynamicrouting":<String_value>,

"mtu":<Integer_value>,

"sharing":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vlan? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"vlan":{

<b>"id":<Integer_value>,

</b>"aliasname":true,

"dynamicrouting":true,
```

```
"ipv6dynamicrouting":true,

"mtu":true,

"sharing":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vlan **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/vlan? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/vlan? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of vlan resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/vlan? **view=summary**

Use this query-parameter to get the summary output of vlan resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/vlan? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vlan resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vlan": [ {

"id":<Integer_value>,

"aliasname":<String_value>,

"linklocalipv6addr":<String_value>,

"rnat":<Boolean_value>,

"portbitmap":<Integer_value>,

"lsbitmap":<Integer_value>,

"tagbitmap":<Integer_value>,

"lstagbitmap":<Integer_value>,

"ifaces":<String_value>,

"tagifaces":<String_value>,

"dynamicrouting":<String_value>,

"ipv6dynamicrouting":<String_value>,

"ifnum":<String_value>,

"tagged":<Boolean_value>,

"vlantd":<Integer_value>,

"sdxvlan":<String_value>,
```

```
"mtu":<Integer_value>,

"sharing":<String_value>,

"partitionname":<String_value>,

"vxlan":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vlan/ id_value<Integer> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/vlan/ id_value<Integer> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/vlan/ id_value<Integer> ? **view=summary**

Use this query-parameter to get the summary output of vlan resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vlan": [ {

"id":<Integer_value>,

"aliasname":<String_value>,

"linklocalipv6addr":<String_value>,

"rnat":<Boolean_value>,

"portbitmap":<Integer_value>,

"lsbitmap":<Integer_value>,

"tagbitmap":<Integer_value>,

"lstagbitmap":<Integer_value>,

"ifaces":<String_value>,

"tagifaces":<String_value>,

"dynamicrouting":<String_value>,

"ipv6dynamicrouting":<String_value>,

"ifnum":<String_value>,

"tagged":<Boolean_value>,

"vlantd":<Integer_value>,

"sdxvlan":<String_value>,

"mtu":<Integer_value>,

"sharing":<String_value>,

"partitionname":<String_value>,

"vxlan":<Integer_value>,

"_nextgenapiresource":<String_value>
```

```
}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vlan? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vlan": [ { "__count": "#no"} ] }
```

vlan_binding

Binding object which returns the resources bound to vlan.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
id	<Integer>	Read-write	Integer that uniquely identifies the VLAN for which the details are to be displayed. Minimum value = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum value = 4094
vlan_channel_binding	<vlan_channel_binding[]>	Read-only	channel that can be bound to vlan.
vlan_nsip_binding	<vlan_nsip_binding[]>	Read-only	nsip that can be bound to vlan.
vlan_linkset_binding	<vlan_linkset_binding[]>	Read-only	linkset that can be bound to vlan.
vlan_nsip6_binding	<vlan_nsip6_binding[]>	Read-only	nsip6 that can be bound to vlan.
vlan_interface_binding	<vlan_interface_binding[]>	Read-only	interface that can be bound to vlan.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vlan_binding/ id_value<Integer> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vlan_binding": [ {

"id":<Integer_value>,

"vlan_linkset_binding":<vlan_linkset_binding[]_value>,

"vlan_channel_binding":<vlan_channel_binding[]_value>,

"vlan_nsip6_binding":<vlan_nsip6_binding[]_value>,

"vlan_interface_binding":<vlan_interface_binding[]_value>,
```

```
"vlan_nsip_binding":<vlan_nsip_binding[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vlan_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/vlan_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vlan_binding": [ {

"id":<Integer_value>,

"vlan_linkset_binding":<vlan_linkset_binding[]_value>,

"vlan_channel_binding":<vlan_channel_binding[]_value>,

"vlan_nsip6_binding":<vlan_nsip6_binding[]_value>,

"vlan_interface_binding":<vlan_interface_binding[]_value>,
```

```
"vlan_nsip_binding":<vlan_nsip_binding[]_value>

}]}
```

vlan_channel_binding

Binding object showing the channel that can be bound to vlan.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
tagged	<Boolean>	Read-write	Make the interface an 802.1q tagged interface. Packets sent on this interface on this VLAN have an additional 4-byte 802.1q tag, which identifies the VLAN. To use 802.1q tagging, you must also configure the switch connected to the appliance's interfaces.
ownergroup	<String>	Read-write	The owner node group in a Cluster for this vlan. Default value: DEFAULT_NG Minimum length = 1
id	<Integer>	Read-write	Specifies the virtual LAN ID. Minimum value = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum value = 4094
ifnum	<String>	Read-write	The interface to be bound to the VLAN, specified in slot/port notation (for example, 1/3). Minimum length = 1
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/vlan_channel_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"vlan_channel_binding":{

<b>"id":<Integer_value>,

</b>"ifnum":<String_value>,

"tagged":<Boolean_value>,

"ownergroup":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vlan_channel_binding/ id_value<Integer>
Query-parameters: args http:// <netscaler-ip-address> /nitro/v1/config/vlan_channel_binding/ id_value<Integer> ? **args=ifnum: <String_value> ,tagged: <Boolean_value> ,ownergroup: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vlan_channel_binding/ id_value<Integer>
Query-parameters: filter http:// <netscaler-ip-address> /nitro/v1/config/vlan_channel_binding/ id_value<Integer> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of vlan_channel_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/vlan_channel_binding/ id_value<Integer> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vlan_channel_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vlan_channel_binding": [ {

"tagged":<Boolean_value>,

"ownergroup":<String_value>,

"id":<Integer_value>,

"ifnum":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vlan_channel_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/vlan_channel_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vlan_channel_binding": [ {

"tagged":<Boolean_value>,

"ownergroup":<String_value>,

"id":<Integer_value>,

"ifnum":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vlan_channel_binding/ id_value<Integer> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"vlan_channel_binding": [ { "__count": "#no"} ] }
```

vlan_interface_binding

Binding object showing the interface that can be bound to vlan.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
tagged	<Boolean>	Read-write	Make the interface an 802.1q tagged interface. Packets sent on this interface on this VLAN have an additional 4-byte 802.1q tag, which identifies the VLAN. To use 802.1q tagging, you must also configure the switch connected to the appliance's interfaces.
ifnum	<String>	Read-write	The interface to be bound to the VLAN, specified in slot/port notation (for example, 1/3). Minimum length = 1
id	<Integer>	Read-write	Specifies the virtual LAN ID. Minimum value = 1 Maximum value = 4094
ownergroup	<String>	Read-write	The owner node group in a Cluster for this vlan. Default value: DEFAULT_NG Minimum length = 1
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/vlan_interface_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"vlan_interface_binding":{

<b>"id":<Integer_value>,

</b>"ifnum":<String_value>,

"tagged":<Boolean_value>,

"ownergroup":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vlan_interface_binding/ id_value<Integer>
Query-parameters: args http:// <netscaler-ip-address> /nitro/v1/config/vlan_interface_binding/ id_value<Integer> ? **args=ifnum: <String_value> ,tagged: <Boolean_value> ,ownergroup: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vlan_interface_binding/ id_value<Integer>
Query-parameters: filter http:// <netscaler-ip-address> /nitro/v1/config/vlan_interface_binding/ id_value<Integer> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of vlan_interface_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/vlan_interface_binding/ id_value<Integer> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vlan_interface_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vlan_interface_binding": [ {

"tagged":<Boolean_value>,

"ifnum":<String_value>,

"id":<Integer_value>,

"ownergroup":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vlan_interface_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/vlan_interface_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vlan_interface_binding": [ {

"tagged":<Boolean_value>,

"ifnum":<String_value>,

"id":<Integer_value>,

"ownergroup":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vlan_interface_binding/ id_value<Integer> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"vlan_interface_binding": [ { "__count": "#no"} ] }
```

vlan_linkset_binding

Binding object showing the linkset that can be bound to vlan.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
tagged	<Boolean>	Read-write	Make the interface an 802.1q tagged interface. Packets sent on this interface on this VLAN have an additional 4-byte 802.1q tag, which identifies the VLAN. To use 802.1q tagging, you must

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			also configure the switch connected to the appliance's interfaces.
ifnum	<String>	Read-write	The interface to be bound to the VLAN, specified in slot/port notation (for example, 1/3). Minimum length = 1
ownergroup	<String>	Read-write	The owner node group in a Cluster for this vlan. Default value: DEFAULT_NG Minimum length = 1
id	<Integer>	Read-write	Specifies the virtual LAN ID. Minimum value = 1 Maximum value = 4094
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/vlan_linkset_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"vlan_linkset_binding":{

<b>"id":<Integer_value>,

</b>"ifnum":<String_value>,
```

```
"tagged":<Boolean_value>,

"ownergroup":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vlan_linkset_binding/ id_value<Integer> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/vlan_linkset_binding/ id_value<Integer> ? **args=ifnum: <String_value> ,tagged: <Boolean_value> ,ownergroup: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vlan_linkset_binding/ id_value<Integer> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/vlan_linkset_binding/ id_value<Integer> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of vlan_linkset_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/vlan_linkset_binding/ id_value<Integer> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vlan_linkset_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vlan_linkset_binding": [ {

"tagged":<Boolean_value>,

"ifnum":<String_value>,

"ownergroup":<String_value>,

"id":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vlan_linkset_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/vlan_linkset_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vlan_linkset_binding": [ {

"tagged":<Boolean_value>,

"ifnum":<String_value>,

"ownergroup":<String_value>,

"id":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vlan_linkset_binding/ id_value<Integer> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"vlan_linkset_binding": [ { "__count": "#no"} ] }
```

vlan_nsip6_binding

Binding object showing the nsip6 that can be bound to vlan.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
netmask	<String>	Read-write	Subnet mask for the network address defined for this VLAN. Minimum length = 1
ipaddress	<String>	Read-write	The IP address assigned to the VLAN.
ownergroup	<String>	Read-write	The owner node group in a Cluster for this vlan. Default value: DEFAULT_NG Minimum length = 1
id	<Integer>	Read-write	Specifies the virtual LAN ID. Minimum value = 1 Maximum value = 4094

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
td	<Integer>	Read-write	Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0. Minimum value = 0 Maximum value = 4094
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/vlan_nsip6_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"vlan_nsip6_binding":{

<b>"id":<Integer_value>,

</b>"ipaddress":<String_value>,

"netmask":<String_value>,

"td":<Integer_value>,

"ownergroup":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vlan_nsip6_binding/ id_value<Integer> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/vlan_nsip6_binding/ id_value<Integer> ? **args=ipaddress: <String_value> ,netmask: <String_value> ,td: <Integer_value> ,ownergroup: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vlan_nsip6_binding/ id_value<Integer> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/vlan_nsip6_binding/ id_value<Integer> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of vlan_nsip6_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/vlan_nsip6_binding/ id_value<Integer> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vlan_nsip6_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vlan_nsip6_binding": [ {

"netmask":<String_value>,

"ipaddress":<String_value>,

"ownergroup":<String_value>,

"id":<Integer_value>,

"td":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vlan_nsip6_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/vlan_nsip6_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vlan_nsip6_binding": [ {

"netmask":<String_value>,

"ipaddress":<String_value>,

"ownergroup":<String_value>,

"id":<Integer_value>,

"td":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vlan_nsip6_binding/ id_value<Integer> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"vlan_nsip6_binding": [ { "__count": "#no"} ] }
```

vlan_nsip_binding

Binding object showing the nsip that can be bound to vlan.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
netmask	<String>	Read-write	Subnet mask for the network address defined for this VLAN.
ipaddress	<String>	Read-write	The IP address assigned to the VLAN.
id	<Integer>	Read-write	Specifies the virtual LAN ID. Minimum value = 1 Maximum value = 4094
ownergroup	<String>	Read-write	The owner node group in a Cluster for this vlan. Default value: DEFAULT_NG Minimum length = 1
td	<Integer>	Read-write	Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			an ID, the entity becomes part of the default traffic domain, which has an ID of 0. Minimum value = 0 Maximum value = 4094
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/vlan_nsip_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"vlan_nsip_binding":{

<b>"id":<Integer_value>,

</b>"ipaddress":<String_value>,

"netmask":<String_value>,

"td":<Integer_value>,

"ownergroup":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vlan_nsip_binding/ id_value<Integer> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/vlan_nsip_binding/ id_value<Integer> ? **args=ipaddress: <String_value> ,netmask: <String_value> ,td: <Integer_value> ,ownergroup: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vlan_nsip_binding/ id_value<Integer> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/vlan_nsip_binding/ id_value<Integer> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of vlan_nsip_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/vlan_nsip_binding/ id_value<Integer> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vlan_nsip_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vlan_nsip_binding": [ {

"netmask":<String_value>,

"ipaddress":<String_value>,

"id":<Integer_value>,

"ownergroup":<String_value>,

"td":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vlan_nsip_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/vlan_nsip_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vlan_nsip_binding": [ {

"netmask":<String_value>,

"ipaddress":<String_value>,

"id":<Integer_value>,

"ownergroup":<String_value>,

"td":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vlan_nsip_binding/ id_value<Integer> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"vlan_nsip_binding": [ { "__count": "#no"} ] }
```

vrid

Configuration for Virtual Router ID resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
id	<Integer>	Read-write	Integer that uniquely identifies the VMAC address. The generic VMAC address is in the form of 00:00:5e:00:01:<VRID>. For example, if you add a VRID with a value of 60 and bind it to an interface, the resulting VMAC address is 00:00:5e:00:01:3c, where 3c is the hexadecimal representation of 60. Minimum value = 1 Maximum value = 255
priority	<Integer>	Read-write	Base priority (BP), in an active-active mode configuration, which ordinarily determines the master VIP address. Default value: 255 Minimum value = 0 Maximum value = 255

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
preemption	<String>	Read-write	In an active-active mode configuration, make a backup VIP address the master if its priority becomes higher than that of a master VIP address bound to this VMAC address. If you disable pre-emption while a backup VIP address is the master, the backup VIP address remains master until the original master VIP's priority becomes higher than that of the current master. Default value: ENABLED Possible values = ENABLED, DISABLED
sharing	<String>	Read-write	In an active-active mode configuration, enable the backup VIP address to process any traffic instead of dropping it. Default value: DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ENABLED, DISABLED
tracking	<String>	Read-write	The effective priority (EP) value, relative to the base priority (BP) value in an active-active mode configuration. When EP is set to a value other than None, it is EP, not BP, which determines the master VIP address. Available settings function as follows: * NONE - No tracking. EP = BP * ALL - If the status of all virtual servers is UP, EP = BP. Otherwise, EP = 0. * ONE - If the status of at least one virtual server is UP, EP = BP. Otherwise, EP = 0. * PROGRESSIVE - If the status of all virtual servers is UP, EP = BP. If the status of all virtual servers is DOWN, EP = 0. Otherwise

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			EP = BP (1 - K/N), where N is the total number of virtual servers associated with the VIP address and K is the number of virtual servers for which the status is DOWN. Default: NONE. Default value: NONE Possible values = NONE, ONE, ALL, PROGRESSIVE
ownernode	<Integer>	Read-write	In a cluster setup, assign a cluster node as the owner of this VMAC address for IP based VRRP configuration. If no owner is configured, owner node is displayed as ALL and one node is dynamically elected as the owner. Minimum value = 0 Maximum value = 31
trackifnumpriority	<Integer>	Read-write	Priority by which the Effective priority will be reduced if any of

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			the tracked interfaces goes down in an active-active configuration. Default value: 0 Minimum value = 1 Maximum value = 255
preemptiondelaytimer	<Integer>	Read-write	Preemption delay time, in seconds, in an active-active configuration. If any high priority node will come in network, it will wait for these many seconds before becoming master. Default value: 0 Minimum value = 1 Maximum value = 36000
all	<Boolean>	Read-write	Remove all the configured VMAC addresses from the Citrix ADC.
ifaces	<String>	Read-only	Interfaces bound to this VRID.
type	<String>	Read-only	Indicates whether this VRID entry was added manually or dynamically. When you manually add a VRID entry, the value

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			for this parameter is STATIC. Otherwise, it is DYNAMIC. Possible values = STATIC, DYNAMIC
effectivepriority	<Integer>	Read-only	The effective priority of this VRID.
flags	<Integer>	Read-only	Flags.
ipaddress	<String>	Read-only	The IP address bound to the VRID.
state	<Integer>	Read-only	State of this VRID.
operationalownernode	<Integer>	Read-only	Run time owner node of the vrid. Minimum value = 0 Maximum value = 31
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/vrid **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"vrid":{

<b>"id":<Integer_value>,

</b>"priority":<Integer_value>,
```

```
"preemption":<String_value>,

"sharing":<String_value>,

"tracking":<String_value>,

"ownernode":<Integer_value>,

"trackifnumpriority":<Integer_value>,

"preemptiondelaytimer":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vrid/ id_value<Integer> **Query-parameters: args=all: <Boolean_value>**
update
URL: http:// <netscaler-ip-address> /nitro/v1/config/vrid **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"vrid":{

<b>"id":<Integer_value>,

</b>"priority":<Integer_value>,

"preemption":<String_value>,
```

```
"sharing":<String_value>,

"tracking":<String_value>,

"ownernode":<Integer_value>,

"trackifnumpriority":<Integer_value>,

"preemptiondelaytimer":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

unset

URL: http:// <netscaler-ip-address> /nitro/v1/config/vrid? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"vrid":{

<b>"id":<Integer_value>,

</b>"priority":true,

"preemption":true,

"sharing":true,

"tracking":true,

"ownernode":true,
```

```
"trackifnumpriority":true,

"preemptiondelaytimer":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error
get (all)
URL: http:// <netscaler-ip-address> /nitro/v1/config/vrid **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/vrid? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/vrid? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of vrid resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/vrid? **view=summary**

Use this query-parameter to get the summary output of vrid resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/vrid? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vrid resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vrid": [ {

"id":<Integer_value>,

"ifaces":<String_value>,

"type":<String_value>,

"priority":<Integer_value>,

"effectivepriority":<Integer_value>,

"preemption":<String_value>,

"sharing":<String_value>,

"tracking":<String_value>,

"flags":<Integer_value>,

"ipaddress":<String_value>,

"state":<Integer_value>,

"operationalownernode":<Integer_value>,

"ownernode":<Integer_value>,

"trackifnumpriority":<Integer_value>,

"preemptiondelaytimer":<Integer_value>,

"_nextgenapiresource":<String_value>
```

```
}]}
```

get

URL: http:// <netscaler-ip-address> /nitro/v1/config/vrid/ id_value<Integer> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/vrid/ id_value<Integer> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/vrid/ id_value<Integer> ? **view=summary**

Use this query-parameter to get the summary output of vrid resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vrid": [ {

"id":<Integer_value>,

"ifaces":<String_value>,

"type":<String_value>,
```

```
"priority":<Integer_value>,

"effectivepriority":<Integer_value>,

"preemption":<String_value>,

"sharing":<String_value>,

"tracking":<String_value>,

"flags":<Integer_value>,

"ipaddress":<String_value>,

"state":<Integer_value>,

"operationalownernode":<Integer_value>,

"ownernode":<Integer_value>,

"trackifnumpriority":<Integer_value>,

"preemptiondelaytimer":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

count

URL: http:// <netscaler-ip-address> /nitro/v1/config/vrid? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vrid": [ { "__count": "#no"} ] }
```

vrid6

Configuration for Virtual Router ID for IPv6 resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
id	<Integer>	Read-write	Integer value that uniquely identifies a VMAC6 address. Minimum value = 1 Maximum value = 255
priority	<Integer>	Read-write	Base priority (BP), in an active-active mode configuration, which ordinarily determines the master VIP address. Default value: 255 Minimum value = 0 Maximum value = 255
preemption	<String>	Read-write	In an active-active mode configuration, make a backup VIP address the master if

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			its priority becomes higher than that of a master VIP address bound to this VMAC address. If you disable pre-emption while a backup VIP address is the master, the backup VIP address remains master until the original master VIP's priority becomes higher than that of the current master. Default value: ENABLED Possible values = ENABLED, DISABLED
sharing	<String>	Read-write	In an active-active mode configuration, enable the backup VIP address to process any traffic instead of dropping it. Default value: DISABLED Possible values = ENABLED, DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
tracking	<String>	Read-write	The effective priority (EP) value, relative to the base priority (BP) value in an active-active mode configuration. When EP is set to a value other than None, it is EP, not BP, which determines the master VIP address. Available settings function as follows: * NONE - No tracking. EP = BP * ALL - If the status of all virtual servers is UP, EP = BP. Otherwise, EP = 0. * ONE - If the status of at least one virtual server is UP, EP = BP. Otherwise, EP = 0. * PROGRESSIVE - If the status of all virtual servers is UP, EP = BP. If the status of all virtual servers is DOWN, EP = 0. Otherwise EP = BP (1 - K/N), where N is the total number of virtual servers associated

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			with the VIP address and K is the number of virtual servers for which the status is DOWN. Default: NONE. Default value: NONE Possible values = NONE, ONE, ALL, PROGRESSIVE
preemptiondelaytimer	<Integer>	Read-write	Preemption delay time in seconds, in an active-active configuration. If any high priority node will come in network, it will wait for these many seconds before becoming master. Default value: 0 Minimum value = 1 Maximum value = 36000
trackifnumpriority	<Integer>	Read-write	Priority by which the Effective priority will be reduced if any of the tracked interfaces goes down in an active-active configuration.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: 0 Minimum value = 1 Maximum value = 255
ownernode	<Integer>	Read-write	In a cluster setup, assign a cluster node as the owner of this VMAC address for IP based VRRP configuration. If no owner is configured, ow ner node is displayed as ALL and one node is dynamically elected as the owner. Minimum value = 0 Maximum value = 31
all	<Boolean>	Read-write	Remove all configured VMAC6 addresses from the Citrix ADC.
ifaces	<String>	Read-only	Interfaces bound to this VRID.
ifnum	<String>	Read-only	Interfaces to bind to the VMAC6, specified in (slot/port) notation (for example, 1/2).Use spaces to separate multiple entries.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
type	<String>	Read-only	Type (static or dynamic) of this VRID. Possible values = STATIC, DYNAMIC
state	<Integer>	Read-only	State of this VRID.
flags	<Integer>	Read-only	Flags.
ipaddress	<String>	Read-only	The IP address bound to the VRID6.
effectivepriority	<Integer>	Read-only	The effective priority of this VRID.
operationalownernode	<Integer>	Read-only	Run time owner node of the vrid. Minimum value = 0 Maximum value = 31
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/vrid6 **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"vrid6":{

<b>"id":<Integer_value>,

</b>"priority":<Integer_value>,
```

```
"preemption":<String_value>,

"sharing":<String_value>,

"tracking":<String_value>,

"preemptiondelaytimer":<Integer_value>,

"trackifnumpriority":<Integer_value>,

"ownernode":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vrid6/ id_value<Integer> **Query-parameters: args=all: <Boolean_value>**
update
URL: http:// <netscaler-ip-address> /nitro/v1/config/vrid6 **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"vrid6":{

<b>"id":<Integer_value>,

</b>"priority":<Integer_value>,

"preemption":<String_value>,
```

```
"sharing":<String_value>,

"tracking":<String_value>,

"preemptiondelaytimer":<Integer_value>,

"trackifnumpriority":<Integer_value>,

"ownernode":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

unset

URL: http:// <netscaler-ip-address> /nitro/v1/config/vrid6? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"vrid6":{

<b>"id":<Integer_value>,

</b>"priority":true,

"preemption":true,

"sharing":true,

"tracking":true,

"preemptiondelaytimer":true,
```

```
"trackifnumpriority":true,

"ownernode":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error
get (all)
URL: http:// <netscaler-ip-address> /nitro/v1/config/vrid6 **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/vrid6? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/vrid6? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of vrid6 resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/vrid6? **view=summary**

Use this query-parameter to get the summary output of vrid6 resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/vrid6? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vrid6 resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vrid6": [ {

"id":<Integer_value>,

"ifaces":<String_value>,

"ifnum":<String_value>,

"type":<String_value>,

"priority":<Integer_value>,

"state":<Integer_value>,

"flags":<Integer_value>,

"ipaddress":<String_value>,

"preemption":<String_value>,

"sharing":<String_value>,

"preemptiondelaytimer":<Integer_value>,

"trackifnumpriority":<Integer_value>,

"effectivepriority":<Integer_value>,

"tracking":<String_value>,

"operationalownernode":<Integer_value>,

"ownernode":<Integer_value>,
```

```
"_nextgenapiresource":<String_value>

}]}
```

get
URL: http:// <netscaler-ip-address> /nitro/v1/config/vrid6/ id_value<Integer> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/vrid6/ id_value<Integer> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/vrid6/ id_value<Integer> ? **view=summary**

Use this query-parameter to get the summary output of vrid6 resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vrid6": [ {

"id":<Integer_value>,

"ifaces":<String_value>,
```

```
"ifnum":<String_value>,

"type":<String_value>,

"priority":<Integer_value>,

"state":<Integer_value>,

"flags":<Integer_value>,

"ipaddress":<String_value>,

"preemption":<String_value>,

"sharing":<String_value>,

"preemptiondelaytimer":<Integer_value>,

"trackifnumpriority":<Integer_value>,

"effectivepriority":<Integer_value>,

"tracking":<String_value>,

"operationalownernode":<Integer_value>,

"ownernode":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

count

URL: http:// <netscaler-ip-address> /nitro/v1/config/vrid6? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vrid6": [ { "__count": "#no"} ] }
```

vrid6_binding

Binding object which returns the resources bound to vrid6.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
id	<Integer>	Read-write	Integer value that uniquely identifies a VMAC6 address. Minimum value = 1 Maximum value = 255
vrid6_nsip_binding	<vrid6_nsip_binding[]>	Read-only	nsip that can be bound to vrid6.
vrid6_nsip6_binding	<vrid6_nsip6_binding[]>	Read-only	nsip6 that can be bound to vrid6.
vrid6_channel_binding	<vrid6_channel_binding[]>	Read-only	channel that can be bound to vrid6.
vrid6_trackinterface_binding	<vrid6_trackinterface_binding[]>	Read-only	trackinterface that can be bound to vrid6.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
vrid6_interface_binding	<vrid6_interface_binding[]>	Read-only	interface that can be bound to vrid6.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vrid6_binding/ id_value<Integer> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vrid6_binding": [ {

"id":<Integer_value>,

"vrid6_nsip_binding":<vrid6_nsip_binding[]_value>,

"vrid6_nsip6_binding":<vrid6_nsip6_binding[]_value>,

"vrid6_interface_binding":<vrid6_interface_binding[]_value>,

"vrid6_trackinterface_binding":<vrid6_trackinterface_binding[]_value>,

"vrid6_channel_binding":<vrid6_channel_binding[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vrid6_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/vrid6_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vrid6_binding": [ {

"id":<Integer_value>,

"vrid6_nsip_binding":<vrid6_nsip_binding[]_value>,

"vrid6_nsip6_binding":<vrid6_nsip6_binding[]_value>,

"vrid6_interface_binding":<vrid6_interface_binding[]_value>,

"vrid6_trackinterface_binding":<vrid6_trackinterface_binding[]_value>,

"vrid6_channel_binding":<vrid6_channel_binding[]_value>

}]}
```

vrid6_channel_binding

Binding object showing the channel that can be bound to vrid6.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
id	<Integer>	Read-write	Integer value that uniquely identifies a VMAC6 address. Minimum value = 1 Maximum value = 255
ifnum	<String>	Read-write	Interfaces to bind to the VMAC6, specified in (slot/port) notation (for example, 1/2).Use spaces to separate multiple entries.
vlan	<Integer>	Read-only	The VLAN in which this VRID resides.
flags	<Integer>	Read-only	Flags.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/vrid6_channel_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"vrid6_channel_binding":{

<b>"id":<Integer_value>,

</b>"ifnum":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vrid6_channel_binding/ id_value<Integer>
Query-parameters: args http:// <netscaler-ip-address> /nitro/v1/config/vrid6_channel_binding/ id_value<Integer> ? **args=ifnum: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vrid6_channel_binding/ id_value<Integer>
Query-parameters: filter http:// <netscaler-ip-address> /nitro/v1/config/vrid6_channel_binding/ id_value<Integer> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of vrid6_channel_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/vrid6_channel_binding/ id_value<Integer> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vrid6_channel_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vrid6_channel_binding": [ {

"id":<Integer_value>,

"ifnum":<String_value>,

"vlan":<Integer_value>,

"flags":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vrid6_channel_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/vrid6_channel_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vrid6_channel_binding": [ {

"id":<Integer_value>,

"ifnum":<String_value>,

"vlan":<Integer_value>,

"flags":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vrid6_channel_binding/ id_value<Integer> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"vrid6_channel_binding": [ { "__count": "#no"} ] }
```

vrid6_interface_binding

Binding object showing the interface that can be bound to vrid6.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ifnum	<String>	Read-write	Interfaces to bind to the VMAC6, specified in (slot/port) notation (for example, 1/2).Use spaces to separate multiple entries.
id	<Integer>	Read-write	Integer value that uniquely identifies a VMAC6 address. Minimum value = 1 Maximum value = 255
flags	<Integer>	Read-only	Flags.
vlan	<Integer>	Read-only	The VLAN in which this VRID resides.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/vrid6_interface_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"vrid6_interface_binding":{

<b>"id":<Integer_value>,

</b>"ifnum":<String_value>
```

```
}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vrid6_interface_binding/ id_value<Integer>
Query-parameters: args http:// <netscaler-ip-address> /nitro/v1/config/vrid6_interface_binding/ id_value<Integer> ? **args=ifnum: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vrid6_interface_binding/ id_value<Integer>
Query-parameters: filter http:// <netscaler-ip-address> /nitro/v1/config/vrid6_interface_binding/ id_value<Integer> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of vrid6_interface_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/vrid6_interface_binding/ id_value<Integer> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vrid6_interface_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vrid6_interface_binding": [ {

"ifnum":<String_value>,

"id":<Integer_value>,

"flags":<Integer_value>,

"vlan":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vrid6_interface_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/vrid6_interface_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vrid6_interface_binding": [ {

"ifnum":<String_value>,

"id":<Integer_value>,

"flags":<Integer_value>,

"vlan":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vrid6_interface_binding/ id_value<Integer> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"vrid6_interface_binding": [ { "__count": "#no"} ] }
```

vrid6_nsip6_binding

Binding object showing the nsip6 that can be bound to vrid6.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
id	<Integer>	Read-write	Integer value that uniquely identifies a VMAC6 address. Minimum value = 1 Maximum value = 255
ipaddress	<String>	Read-write	The IP address bound to the VRID6.
flags	<Integer>	Read-only	Flags.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vrid6_nsip6_binding/ id_value<Integer> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/vrid6_nsip6_binding/ id_value<Integer> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of vrid6_nsip6_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/vrid6_nsip6_binding/ id_value<Integer> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vrid6_nsip6_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vrid6_nsip6_binding": [ {

"id":<Integer_value>,

"ipaddress":<String_value>,

"flags":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vrid6_nsip6_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/vrid6_nsip6_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vrid6_nsip6_binding": [ {

"id":<Integer_value>,

"ipaddress":<String_value>,

"flags":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vrid6_nsip6_binding/ id_value<Integer> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"vrid6_nsip6_binding": [ { "__count": "#no"} ] }
```

vrid6_nsip_binding

Binding object showing the nsip that can be bound to vrid6.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
id	<Integer>	Read-write	Integer value that uniquely identifies a VMAC6 address. Minimum value = 1 Maximum value = 255
ipaddress	<String>	Read-write	The IP address bound to the VRID6.
flags	<Integer>	Read-only	Flags.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vrid6_nsip_binding/ id_value<Integer> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/vrid6_nsip_binding/ id_value<Integer> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of vrid6_nsip_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/vrid6_nsip_binding/ id_value<Integer> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vrid6_nsip_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vrid6_nsip_binding": [ {

"id":<Integer_value>,
```

```
"ipaddress":<String_value>,

"flags":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vrid6_nsip_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/vrid6_nsip_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vrid6_nsip_binding": [ {

"id":<Integer_value>,

"ipaddress":<String_value>,

"flags":<Integer_value>

}]}
```

```
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vrid6_nsip_binding/ id_value<Integer> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"vrid6_nsip_binding": [ { "__count": "#no"} ] }
```

vrid6_trackinterface_binding

Binding object showing the trackinterface that can be bound to vrid6.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
trackifnum	<String>	Read-write	Interfaces which need to be tracked for this vrID.
id	<Integer>	Read-write	Integer value that uniquely identifies a VMAC6 address.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum value = 1 Maximum value = 255
flags	<Integer>	Read-only	Flags.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/vrid6_trackinterface_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"vrid6_trackinterface_binding":{

<b>"id":<Integer_value>,

</b>"trackifnum":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vrid6_trackinterface_binding/ id_value<Integer> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ vrid6_trackinterface_binding/ id_value<Integer> ? **args=trackifnum: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vrid6_trackinterface_binding/ id_value<Integer>
Query-parameters: filter http:// <netscaler-ip-address> /nitro/v1/config/ vrid6_trackinterface_binding/ id_value<Integer> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of vrid6_trackinterface_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/vrid6_trackinterface_binding/ id_value<Integer> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vrid6_trackinterface_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vrid6_trackinterface_binding": [ {

"trackifnum":<String_value>,

"id":<Integer_value>,
```

```
"flags":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vrid6_trackinterface_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/vrid6_trackinterface_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vrid6_trackinterface_binding": [ {

"trackifnum":<String_value>,

"id":<Integer_value>,

"flags":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vrid6_trackinterface_binding/ id_value<Integer> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"vrid6_trackinterface_binding": [ { "__count": "#no"} ] }
```

vrid_binding

Binding object which returns the resources bound to vrid.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
id	<Integer>	Read-write	Integer value that uniquely identifies the VMAC address. Minimum value = 1 Maximum value = 255

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
vrid_interface_binding	<vrid_interface_binding[]>	Read-only	interface that can be bound to vrid.
vrid_trackinterface_binding	<vrid_trackinterface_binding[]>	Read-only	trackinterface that can be bound to vrid.
vrid_channel_binding	<vrid_channel_binding[]>	Read-only	channel that can be bound to vrid.
vrid_nsip6_binding	<vrid_nsip6_binding[]>	Read-only	nsip6 that can be bound to vrid.
vrid_nsip_binding	<vrid_nsip_binding[]>	Read-only	nsip that can be bound to vrid.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vrid_binding/ id_value<Integer> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vrid_binding": [ {

"id":<Integer_value>,

"vrid_nsip_binding":<vrid_nsip_binding[]_value>,

"vrid_interface_binding":<vrid_interface_binding[]_value>,

"vrid_channel_binding":<vrid_channel_binding[]_value>,

"vrid_nsip6_binding":<vrid_nsip6_binding[]_value>,

"vrid_trackinterface_binding":<vrid_trackinterface_binding[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vrid_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/vrid_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vrid_binding": [ {

"id":<Integer_value>,

"vrid_nsip_binding":<vrid_nsip_binding[]_value>,

"vrid_interface_binding":<vrid_interface_binding[]_value>,

"vrid_channel_binding":<vrid_channel_binding[]_value>,

"vrid_nsip6_binding":<vrid_nsip6_binding[]_value>,

"vrid_trackinterface_binding":<vrid_trackinterface_binding[]_value>

}]}
```

vrid_channel_binding

Binding object showing the channel that can be bound to vrid.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ifnum	<String>	Read-write	Interfaces to bind to the VMAC, specified in (slot/port) notation (for example, 1/2).Use spaces to separate multiple entries.
id	<Integer>	Read-write	Integer that uniquely identifies the VMAC address. The generic VMAC address is in the form of 00:00:5e:00:01:<VRID>. For example, if you add a VRID with a value of 60 and bind it to an interface, the resulting VMAC address is 00:00:5e:00:01:3c, where 3c is the hexadecimal representation of 60. Minimum value = 1 Maximum value = 255

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
vlan	<Integer>	Read-only	The VLAN in which this VRID resides.
flags	<Integer>	Read-only	Flags.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/vrid_channel_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"vrid_channel_binding":{

<b>"id":<Integer_value>,

</b>"ifnum":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vrid_channel_binding/ id_value<Integer> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/vrid_channel_binding/ id_value<Integer> ? **args=ifnum: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vrid_channel_binding/ id_value<Integer>
Query-parameters: filter http:// <netscaler-ip-address> /nitro/v1/config/vrid_channel_binding/ id_value<Integer> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of vrid_channel_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/vrid_channel_binding/ id_value<Integer> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vrid_channel_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vrid_channel_binding": [ {

"ifnum":<String_value>,

"id":<Integer_value>,

"vlan":<Integer_value>,

"flags":<Integer_value>
```

```
}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vrid_channel_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/vrid_channel_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vrid_channel_binding": [ {

"ifnum":<String_value>,

"id":<Integer_value>,

"vlan":<Integer_value>,

"flags":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vrid_channel_binding/ id_value<Integer> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"vrid_channel_binding": [ { "__count": "#no"} ] }
```

vrid_interface_binding

Binding object showing the interface that can be bound to vrid.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ifnum	<String>	Read-write	Interfaces to bind to the VMAC, specified in (slot/port) notation (for example, 1/2).Use spaces to separate multiple entries.
id	<Integer>	Read-write	Integer that uniquely identifies the VMAC

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			address. The generic VMAC address is in the form of 00:00:5e:00:01:<VRID>. For example, if you add a VRID with a value of 60 and bind it to an interface, the resulting VMAC address is 00:00:5e:00:01:3c, where 3c is the hexadecimal representation of 60. Minimum value = 1 Maximum value = 255
vlan	<Integer>	Read-only	The VLAN in which this VRID resides.
flags	<Integer>	Read-only	Flags.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/vrid_interface_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"vrid_interface_binding":{

<b>"id":<Integer_value>,

</b>"ifnum":<String_value>
```

```
}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vrid_interface_binding/ id_value<Integer>
Query-parameters: args http:// <netscaler-ip-address> /nitro/v1/config/vrid_interface_binding/ id_value<Integer> ? **args=ifnum: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vrid_interface_binding/ id_value<Integer>
Query-parameters: filter http:// <netscaler-ip-address> /nitro/v1/config/vrid_interface_binding/ id_value<Integer> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of vrid_interface_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/vrid_interface_binding/ id_value<Integer> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vrid_interface_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vrid_interface_binding": [ {

"ifnum":<String_value>,

"id":<Integer_value>,

"vlan":<Integer_value>,

"flags":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vrid_interface_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/vrid_interface_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vrid_interface_binding": [ {

"ifnum":<String_value>,

"id":<Integer_value>,

"vlan":<Integer_value>,

"flags":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vrid_interface_binding/ id_value<Integer> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"vrid_interface_binding": [ { "__count": "#no"} ] }
```

vrid_nsip6_binding

Binding object showing the nsip6 that can be bound to vrid.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ipaddress	<String>	Read-write	The IP address bound to the VRID.
id	<Integer>	Read-write	Integer that uniquely identifies the VMAC address. The generic VMAC address is in the form of 00:00:5e:00:01:<VRID>. For example, if you add a VRID with a value of 60 and bind it to an interface, the resulting VMAC address is 00:00:5e:00:01:3c, where 3c is the hexadecimal representation of 60. Minimum value = 1 Maximum value = 255
flags	<Integer>	Read-only	Flags.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.
- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vrid_nsip6_binding/ id_value<Integer> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/vrid_nsip6_binding/ id_value<Integer> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of vrid_nsip6_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/vrid_nsip6_binding/ id_value<Integer> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vrid_nsip6_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vrid_nsip6_binding": [ {

"ipaddress":<String_value>,

"id":<Integer_value>,

"flags":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vrid_nsip6_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ vrid_nsip6_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vrid_nsip6_binding": [ {

"ipaddress":<String_value>,

"id":<Integer_value>,

"flags":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vrid_nsip6_binding/ id_value<Integer> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"vrid_nsip6_binding": [ { "__count": "#no"} ] }
```

vrid_nsip_binding

Binding object showing the nsip that can be bound to vrid.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
id	<Integer>	Read-write	Integer that uniquely identifies the VMAC address. The generic VMAC address is in the form of 00:00:5e:00:01:<VRID>. For example, if you add a VRID with a value of 60 and bind it to an interface, the resulting VMAC address is 00:00:5e:00:01:3c, where 3c is the hexadecimal representation of 60. Minimum value = 1 Maximum value = 255
ipaddress	<String>	Read-write	The IP address bound to the VRID.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
flags	<Integer>	Read-only	Flags.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vrid_nsip_binding/ id_value<Integer> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/vrid_nsip_binding/ id_value<Integer> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of vrid_nsip_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/vrid_nsip_binding/ id_value<Integer> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vrid_nsip_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vrid_nsip_binding": [ {

"id":<Integer_value>,

"ipaddress":<String_value>,

"flags":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vrid_nsip_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/vrid_nsip_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vrid_nsip_binding": [ {

"id":<Integer_value>,

"ipaddress":<String_value>,

"flags":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vrid_nsip_binding/ id_value<Integer> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"vrid_nsip_binding": [ { "__count": "#no"} ] }
```

vrid_trackinterface_binding

Binding object showing the trackinterface that can be bound to vrid.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
trackifnum	<String>	Read-write	Interfaces which need to be tracked for this vrID.
id	<Integer>	Read-write	Integer that uniquely identifies the VMAC address. The generic VMAC address is in the form of 00:00:5e:00:01:<VRID>. For example, if you add a VRID with a value of 60 and bind it to an interface, the resulting VMAC

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			address is 00:00:5e:00:01:3c, where 3c is the hexadecimal representation of 60. Minimum value = 1 Maximum value = 255
flags	<Integer>	Read-only	Flags.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/vrid_trackinterface_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"vrid_trackinterface_binding":{

<b>"id":<Integer_value>,

</b>"trackifnum":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vrid_trackinterface_binding/ id_value<Integer> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ vrid_trackinterface_binding/ id_value<Integer> ? **args=trackifnum: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vrid_trackinterface_binding/ id_value<Integer>
Query-parameters: filter http:// <netscaler-ip-address> /nitro/v1/config/ vrid_trackinterface_binding/ id_value<Integer> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of vrid_trackinterface_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/vrid_trackinterface_binding/ id_value<Integer> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vrid_trackinterface_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vrid_trackinterface_binding": [ {

"trackifnum":<String_value>,

"id":<Integer_value>,

"flags":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vrid_trackinterface_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/vrid_trackinterface_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vrid_trackinterface_binding": [ {

"trackifnum":<String_value>,
```

```
"id":<Integer_value>,

"flags":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vrid_trackinterface_binding/ id_value<Integer> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"vrid_trackinterface_binding": [ { "__count": "#no"} ] }
```

vridparam

Configuration for VR ID parameter resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
sendtomaster	<String>	Read-write	Forward packets to the master node, in

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			an active-active mode configuration, if the virtual server is in the backup state and sharing is disabled. Default value: DISABLED Possible values = ENABLED, DISABLED
hellointerval	<Integer>	Read-write	Interval, in milliseconds, between vrrp advertisement messages sent to the peer node in active-active mode. Default value: 1000 Minimum value = 200 Maximum value = 1000
deadinterval	<Integer>	Read-write	Number of seconds after which a peer node in active-active mode is marked down if vrrp advertisements are not received from the peer node. Default value: 3 Minimum value = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum value = 60
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- UPDATE
- UNSET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vridparam **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"vridparam":{

"sendtomaster":<String_value>,

"hellointerval":<Integer_value>,

"deadinterval":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vridparam? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"vridparam":{

"sendtomaster":true,
```

```
"hellointerval":true,

"deadinterval":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vridparam **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vridparam": [ {

"sendtomaster":<String_value>,

"hellointerval":<Integer_value>,

"deadinterval":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

vxlan

Configuration for "VXLAN" resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
id	<Integer>	Read-write	A positive integer, which is also called VXLAN Network Identifier (VNI), that uniquely identifies a VXLAN. Minimum value = 1 Maximum value = 16777215
vlan	<Integer>	Read-write	ID of VLANs whose traffic is allowed over this VXLAN. If you do not specify any VLAN IDs, the Citrix ADC allows traffic of all VLANs that are not part of any other VXLANs. Minimum value = 2 Maximum value = 4094
port	<Integer>	Read-write	Specifies UDP destination port for VXLAN packets. Default value: 4789 Minimum value = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum value = 65534
dynamicrouting	<String>	Read-write	Enable dynamic routing on this VXLAN. Default value: DISABLED Possible values = ENABLED, DISABLED
ipv6dynamicrouting	<String>	Read-write	Enable all IPv6 dynamic routing protocols on this VXLAN. Note: For the ENABLED setting to work, you must configure IPv6 dynamic routing protocols from the VTYSH command line. Default value: DISABLED Possible values = ENABLED, DISABLED
type	<String>	Read-write	VXLAN encapsulation type. VXLAN, VXLANGPE. Default value: VXLAN

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = VXLAN, VXLANGPE
protocol	<String>	Read-write	VXLAN-GPE next protocol. RESERVED, IPv4, IPv6, ETHERNET, NSH. Default value: ETHERNET Possible values = IPv4, IPv6, ETHERNET, NSH
innervlantagging	<String>	Read-write	Specifies whether Citrix ADC should generate VXLAN packets with inner VLAN tag. Default value: DISABLED Possible values = ENABLED, DISABLED
td	<Integer>	Read-only	Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
partitionname	<String>	Read-only	The Partition to which this vxlan is bound. Minimum length = 1
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/vxlan **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"vxlan":{

<b>"id":<Integer_value>,

</b>"vlan":<Integer_value>,

"port":<Integer_value>,

"dynamicrouting":<String_value>,

"ipv6dynamicrouting":<String_value>,

"type":<String_value>,

"protocol":<String_value>,

"innervlantagging":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vxlan/ id_value<Integer> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vxlan **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"vxlan":{

<b>"id":<Integer_value>,

</b>"vlan":<Integer_value>,

"port":<Integer_value>,

"dynamicrouting":<String_value>,

"ipv6dynamicrouting":<String_value>,

"innervlantagging":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vxlan? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"vxlan":{

<b>"id":<Integer_value>,

</b>"vlan":true,

"port":true,

"dynamicrouting":true,

"ipv6dynamicrouting":true,

"innervlantagging":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vxlan **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/vxlan? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/vxlan? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of vxlan resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/vxlan? **view=summary**

Use this query-parameter to get the summary output of vxlan resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/vxlan? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vxlan resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vxlan": [ {

"id":<Integer_value>,

"vlan":<Integer_value>,

"port":<Integer_value>,

"dynamicrouting":<String_value>,
```

```
"ipv6dynamicrouting":<String_value>,

"innervlantagging":<String_value>,

"td":<Integer_value>,

"type":<String_value>,

"protocol":<String_value>,

"partitionname":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vxlan/ id_value<Integer> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/vxlan/ id_value<Integer> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/vxlan/ id_value<Integer> ? **view=summary**

Use this query-parameter to get the summary output of vxlan resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vxlan": [ {

"id":<Integer_value>,

"vlan":<Integer_value>,

"port":<Integer_value>,

"dynamicrouting":<String_value>,

"ipv6dynamicrouting":<String_value>,

"innervlantagging":<String_value>,

"td":<Integer_value>,

"type":<String_value>,

"protocol":<String_value>,

"partitionname":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vxlan? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vxlan": [ { "__count": "#no"} ] }
```

vxlan_binding

Binding object which returns the resources bound to vxlan.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
id	<Integer>	Read-write	A positive integer, which is also called VXLAN Network Identifier (VNI), that uniquely identifies a VXLAN. Minimum value = 1 Maximum value = 16777215
vxlan_iptunnel_binding	<vxlan_iptunnel_binding[]>	Read-only	iptunnel that can be bound to vxlan.
vxlan_nsip_binding	<vxlan_nsip_binding[]>	Read-only	nsip that can be bound to vxlan.
vxlan_nsip6_binding	<vxlan_nsip6_binding[]>	Read-only	nsip6 that can be bound to vxlan.
vxlan_srcip_binding	<vxlan_srcip_binding[]>	Read-only	srcip that can be bound to vxlan.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vxlan_binding/ id_value<Integer> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vxlan_binding": [ {

"id":<Integer_value>,

"vxlan_nsip_binding":<vxlan_nsip_binding[]_value>,

"vxlan_iptunnel_binding":<vxlan_iptunnel_binding[]_value>,

"vxlan_srcip_binding":<vxlan_srcip_binding[]_value>,

"vxlan_nsip6_binding":<vxlan_nsip6_binding[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vxlan_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/vxlan_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vxlan_binding": [ {

"id":<Integer_value>,

"vxlan_nsip_binding":<vxlan_nsip_binding[]_value>,

"vxlan_iptunnel_binding":<vxlan_iptunnel_binding[]_value>,

"vxlan_srcip_binding":<vxlan_srcip_binding[]_value>,

"vxlan_nsip6_binding":<vxlan_nsip6_binding[]_value>

}]}
```

vxlan_iptunnel_binding

Binding object showing the iptunnel that can be bound to vxlan.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
id	<Integer>	Read-write	A positive integer, which is also called VXLAN Network Identifier (VNI), that uniquely identifies a VXLAN. Minimum value = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum value = 16777215
tunnel	<String>	Read-write	Specifies the name of the configured tunnel to be associated with this VXLAN.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vxlan_iptunnel_binding/ id_value<Integer>
Query-parameters: filter http:// <netscaler-ip-address> /nitro/v1/config/vxlan_iptunnel_binding/ id_value<Integer> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of vxlan_iptunnel_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/vxlan_iptunnel_binding/ id_value<Integer> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vxlan_iptunnel_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vxlan_iptunnel_binding": [ {

"id":<Integer_value>,

"tunnel":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vxlan_iptunnel_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/vxlan_iptunnel_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vxlan_iptunnel_binding": [ {

"id":<Integer_value>,

"tunnel":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vxlan_iptunnel_binding/ id_value<Integer> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"vxlan_iptunnel_binding": [ { "__count": "#no"} ] }
```

vxlan_nsip6_binding

Binding object showing the nsip6 that can be bound to vxlan.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ipaddress	<String>	Read-write	The IP address assigned to the VXLAN.
id	<Integer>	Read-write	A positive integer, which is also called VXLAN Network Identifier (VNI), that uniquely identifies a VXLAN. Minimum value = 1 Maximum value = 16777215

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
netmask	<String>	Read-write	Subnet mask for the network address defined for this VXLAN. Minimum length = 1
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/vxlan_nsip6_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"vxlan_nsip6_binding":{

<b>"id":<Integer_value>,

</b>"ipaddress":<String_value>,

"netmask":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vxlan_nsip6_binding/ id_value<Integer> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/vxlan_nsip6_binding/ id_value<Integer> ? **args=ipaddress: <String_value> ,netmask: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vxlan_nsip6_binding/ id_value<Integer>
Query-parameters: filter http:// <netscaler-ip-address> /nitro/v1/config/vxlan_nsip6_binding/ id_value<Integer> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of vxlan_nsip6_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/vxlan_nsip6_binding/ id_value<Integer> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vxlan_nsip6_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vxlan_nsip6_binding": [ {

"ipaddress":<String_value>,

"id":<Integer_value>,
```

```
"netmask":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vxlan_nsip6_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/vxlan_nsip6_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vxlan_nsip6_binding": [ {

"ipaddress":<String_value>,

"id":<Integer_value>,

"netmask":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vxlan_nsip6_binding/ id_value<Integer> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"vxlan_nsip6_binding": [ { "__count": "#no"} ] }
```

vxlan_nsip_binding

Binding object showing the nsip that can be bound to vxlan.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
netmask	<String>	Read-write	Subnet mask for the network address defined for this VXLAN.
id	<Integer>	Read-write	A positive integer, which is also called VXLAN Network Identifier (VNI), that

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			uniquely identifies a VXLAN. Minimum value = 1 Maximum value = 16777215
ipaddress	<String>	Read-write	The IP address assigned to the VXLAN.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/vxlan_nsip_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"vxlan_nsip_binding":{

<b>"id":<Integer_value>,

</b>"ipaddress":<String_value>,

"netmask":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vxlan_nsip_binding/ id_value<Integer> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/vxlan_nsip_binding/ id_value<Integer> ? **args=ipaddress: <String_value> ,netmask: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vxlan_nsip_binding/ id_value<Integer> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/vxlan_nsip_binding/ id_value<Integer> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of vxlan_nsip_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/vxlan_nsip_binding/ id_value<Integer> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vxlan_nsip_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vxlan_nsip_binding": [ {

"netmask":<String_value>,

"id":<Integer_value>,

"ipaddress":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vxlan_nsip_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/vxlan_nsip_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vxlan_nsip_binding": [ {

"netmask":<String_value>,
```

```
"id":<Integer_value>,

"ipaddress":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vxlan_nsip_binding/ id_value<Integer> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"vxlan_nsip_binding": [ { "__count": "#no"} ] }
```

vxlan_srcip_binding

Binding object showing the srcip that can be bound to vxlan.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
srcip	<String>	Read-write	The source IP address to use in

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			outgoing vxlan packets. Minimum length = 1
id	<Integer>	Read-write	A positive integer, which is also called VXLAN Network Identifier (VNI), that uniquely identifies a VXLAN. Minimum value = 1 Maximum value = 16777215
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of

creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/vxlan_srcip_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"vxlan_srcip_binding":{

<b>"id":<Integer_value>,

</b>"srcip":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vxlan_srcip_binding/ id_value<Integer> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/vxlan_srcip_binding/ id_value<Integer> ? **args=srcip: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vxlan_srcip_binding/ id_value<Integer> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/vxlan_srcip_binding/ id_value<Integer> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of vxlan_srcip_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/vxlan_srcip_binding/ id_value<Integer> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vxlan_srcip_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vxlan_srcip_binding": [ {

"srcip":<String_value>,

"id":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vxlan_srcip_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/vxlan_srcip_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vxlan_srcip_binding": [ {

"srcip":<String_value>,

"id":<Integer_value>
```

```
}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vxlan_srcip_binding/ id_value<Integer> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"vxlan_srcip_binding": [ { "__count": "#no"} ] }
```

vxlanvlanmap

Configuration for vxlan vlan mapping resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the mapping table. Minimum length = 1
_nextgenapiresource	<String>	Read-only	.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/vxlanvlanmap **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"vxlanvlanmap":{

<b>"name":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vxlanvlanmap/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vxlanvlanmap **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/vxlanvlanmap? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/vxlanvlanmap? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of vxlanvlanmap resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/vxlanvlanmap? **view=summary**

Use this query-parameter to get the summary output of vxlanvlanmap resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/vxlanvlanmap? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vxlanvlanmap resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vxlanvlanmap": [ {

"name":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vxlanvlanmap/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/vxlanvlanmap/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/vxlanvlanmap/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of vxlanvlanmap resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vxlanvlanmap": [ {

"name":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

```
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vxlanvlanmap? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vxlanvlanmap": [ { "__count": "#no"} ] }
```

vxlanvlanmap_binding

Binding object which returns the resources bound to vxlanvlanmap.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the mapping table. Minimum length = 1
vxlanvlanmap_vxlan_binding	<vxlanvlanmap_vxlan_binding[]>	Read-only	vxlan that can be bound to vxlanvlanmap.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vxlanvlanmap_binding/ name_value<String>
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vxlanvlanmap_binding": [ {

"name":<String_value>,

"vxlanvlanmap_vxlan_binding":<vxlanvlanmap_vxlan_binding[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vxlanvlanmap_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/vxlanvlanmap_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vxlanvlanmap_binding": [ {

"name":<String_value>,

"vxlanvlanmap_vxlan_binding":<vxlanvlanmap_vxlan_binding[]_value>

}]}
```

vxlanvlanmap_vxlan_binding

Binding object showing the vxlan that can be bound to vxlanvlanmap.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
vxlan	<Integer>	Read-write	The VXLAN assigned to the vlan inside the cloud. Minimum value = 1 Maximum value = 16777215
name	<String>	Read-write	Name of the mapping table. Minimum length = 1
vlan	<String[]>	Read-write	The vlan id or the range of vlan ids in the on-premise network. Minimum length = 1 Maximum length = 4094
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/vxlanvlanmap_vxlan_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"vxlanvlanmap_vxlan_binding":{

<b>"name":<String_value>,

</b>"vxlan":<Integer_value>,

"vlan":<String[]_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vxlanvlanmap_vxlan_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ vxlanvlanmap_vxlan_binding/ name_value<String> ? **args=vxlan: <Integer_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vxlanvlanmap_vxlan_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/

vxlanvlanmap_vxlan_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of vxlanvlanmap_vxlan_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/vxlanvlanmap_vxlan_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vxlanvlanmap_vxlan_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vxlanvlanmap_vxlan_binding": [ {

"vxlan":<Integer_value>,

"name":<String_value>,

"vlan":<String[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vxlanvlanmap_vxlan_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/vxlanvlanmap_vxlan_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vxlanvlanmap_vxlan_binding": [ {

"vxlan":<Integer_value>,

"name":<String_value>,

"vlan":<String[]_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vxlanvlanmap_vxlan_binding/name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"vxlanvlanmap_vxlan_binding": [ { "__count": "#no"} ] }
```

ns

NS

System/Global level configuration.

NAME	DESCRIPTION
nsacl	Configuration for ACL entry
nsacl6	Configuration for ACL6 entry
nsacls	Configuration for ACL entry
nsacls6	Configuration for ACL6 entry
nsaigwprofile	Configuration for AI GW profile
nsappflowcollector	Configuration for appflowCollector
nsappflowparam	Configuration for appflowParam
nsaptlicense	Configuration for aptlicense
nsassignment	Configuration for assignment
nscapacity	Configuration for capacity

NAME	DESCRIPTION
nscentralmanagementserver	Configuration for centralmanagementserver
nschannelparam	
nsconfig	Configuration for system config
nsconfigview	
nsconnectiontable	Configuration for TCP/IP connection table
nsconsoleloginprompt	Configuration for console prompt
nscqaparam	Configuration for cqaparam
nsdhcpip	Configuration for dhcp IP
nsdhcpparams	Configuration for DHCP parameters
nsdiameter	Configuration for Diameter Parameters
nsencryptionkey	Configuration for encryption key
nsencryptionparams	Configuration for default encryption parameters
nsevents	Configuration for events
nsextension	Configuration for Extension
nsextension_binding	Binding object showing the resources that can be bound to nsextension
nsextension_extensionfunction_binding	Binding object showing the extensionfunction that can be bound to nsextension
nsfeature	Configuration for feature
nshardware	Configuration for hardware

NAME	DESCRIPTION
nshmackey	Configuration for HMAC key
nshostname	Configuration for host name
nshttpparam	Configuration for HTTP parameter
nshttpprofile	Configuration for HTTP profile
nsicapprofile	Configuration for ICAP profile
nsip	Configuration for ip
nsip6	Configuration for ip6
nsjob	Configuration for job
nskeymanagerproxy	Configuration for keymanagerproxy
nslaslicense	Configuration for laslicense
nslicense	Configuration for license
nslicenseactivationdata	Configuration for License activation data
nslicenseparameters	Configuration for licenseparameters
nslicenseproxyserver	Configuration for licenseproxyserver
nslicenseserver	Configuration for licenseserver
nslicenseserverpool	Configuration for licenseserver
nslimitidentifier	Configuration for limit Identifier
nslimitidentifier_binding	Binding object showing the resources that can be bound to nslimitidentifier
nslimitidentifier_nslimitsessions_binding	Binding object showing the nslimitsessions that can be bound to nslimitidentifier

NAME	DESCRIPTION
nslimitselector	Configuration for limit selector
nslimitsessions	Configuration for limit sessions
nsmemrecovery	Configuration for memory recovery operations
nsmgmtparam	Configuration for Management related configuration
nsmigration	Configuration for Migration operation
nsmode	Configuration for ns mode
nsnextgenapi	
nsparam	Configuration for Citrix ADC parameters
nspartition	Configuration for admin partition
nspartition_binding	Binding object showing the resources that can be bound to nspartition
nspartition_bridgegroup_binding	Binding object showing the bridgegroup that can be bound to nspartition
nspartition_vlan_binding	Binding object showing the vlan that can be bound to nspartition
nspartition_vxlan_binding	Binding object showing the vxlan that can be bound to nspartition
nspartitionmac	Configuration for partition MACs
nspbr	Configuration for Policy Based Routing(PBR) entry
nspbr6	Configuration for PBR6 entry

NAME	DESCRIPTION
nspbrs	Configuration for Policy based routing
nsratecontrol	Configuration for rate control
nsrollbackcmd	Configuration for Generate rollback commands
nsrpcnode	Configuration for rpc node
nsrunningconfig	Configuration for running configuration
nssavedconfig	Configuration for last saved configuration
nsservicefunction	Configuration for service Function
nsservicepath	Configuration for service Chain
nsservicepath_binding	Binding object showing the resources that can be bound to nsservicepath
nsservicepath_nsservicefunction_binding	Binding object showing the nsservicefunction that can be bound to nsservicepath
nssimpleacl	Configuration for simple ACL
nssimpleacl6	Configuration for simple ACL6
nssourceroutecachetable	Configuration for Source IP Mac Cache Table.
nsspparams	Configuration for Surge Protection parameter
nsstats	Configuration for stats
nssurgeq	Configuration for surge queue
nstcpbufparam	Configuration for tcp buffer parameter
nstcpparam	Configuration for tcp parameters

NAME	DESCRIPTION
nstcpprofile	Configuration for TCP profile
nstestlicense	Configuration for testlicense
nstimeout	Configuration for timeout
nstimer	Configuration for Timer
nstimer_autoscalepolicy_binding	Binding object showing the autoscalepolicy that can be bound to nstimer
nstimer_binding	Binding object showing the resources that can be bound to nstimer
nstimezone	
nstrafficdomain	Configuration for Traffic Domain
nstrafficdomain_binding	Binding object showing the resources that can be bound to nstrafficdomain
nstrafficdomain_bridgegroup_binding	Binding object showing the bridgegroup that can be bound to nstrafficdomain
nstrafficdomain_vlan_binding	Binding object showing the vlan that can be bound to nstrafficdomain
nstrafficdomain_vxlan_binding	Binding object showing the vxlan that can be bound to nstrafficdomain
nsvariable	Configuration for variable
nsvariablevalues	Configuration for Variable runtime data information
nsversion	Configuration for version
nsvpxparam	Configuration for "VPX"

NAME	DESCRIPTION
nsweblogparam	Configuration for Web log parameters
nsxmlnamespace	Configuration for XML namespace
reboot	
shutdown	

nsacl

Configuration for ACL entry resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
aclname	<String>	Read-write	Name for the extended ACL rule. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Minimum length = 1
aclaction	<String>	Read-write	Action to perform on incoming IPv4 packets that match the extended ACL rule.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Available settings function as follows: * ALLOW - The Citrix ADC processes the packet. * BRIDGE - The Citrix ADC bridges the packet to the destination without processing it. * DENY - The Citrix ADC drops the packet. Possible values = BRIDGE, DENY, ALLOW
td	<Integer>	Read-write	Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0. Minimum value = 0 Maximum value = 4094
srcip	<Boolean>	Read-write	IP address or range of IP addresses to

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			match against the source IP address of an incoming IPv4 packet. In the command line interface, separate the range with a hyphen. For example: 10.102.29.30-10.102.29.189.
srcipop	<String>	Read-write	Either the equals (=) or does not equal (!=) logical operator. Possible values = =, !=, EQ, NEQ
srcipval	<String>	Read-write	IP address or range of IP addresses to match against the source IP address of an incoming IPv4 packet. In the command line interface, separate the range with a hyphen. For example:10.102.29.30-10.102.29.189.
srcipdataset	<String>	Read-write	Policy dataset which can have multiple IP ranges bound to it.
srcport	<Boolean>	Read-write	Port number or range of port numbers to match against the source port number of an incoming IPv4

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			packet. In the command line interface, separate the range with a hyphen. For example: 40-90.
srcportop	<String>	Read-write	Either the equals (=) or does not equal (!=) logical operator. Possible values = =, !=, EQ, NEQ
srcportval	<String>	Read-write	Port number or range of port numbers to match against the source port number of an incoming IPv4 packet. In the command line interface, separate the range with a hyphen. For example: 40-90. Maximum length = 65535
srcportdataset	<String>	Read-write	Policy dataset which can have multiple port ranges bound to it.
destip	<Boolean>	Read-write	IP address or range of IP addresses to match against the destination IP address of an incoming IPv4 packet. In the command line

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			interface, separate the range with a hyphen. For example: 10.102.29.30-10.102.29.189.
destipop	<String>	Read-write	Either the equals (=) or does not equal (!=) logical operator. Possible values = =, !=, EQ, NEQ
destipval	<String>	Read-write	IP address or range of IP addresses to match against the destination IP address of an incoming IPv4 packet. In the command line interface, separate the range with a hyphen. For example: 10.102.29.30-10.102.29.189.
destipdataset	<String>	Read-write	Policy dataset which can have multiple IP ranges bound to it.
destport	<Boolean>	Read-write	Port number or range of port numbers to match against the destination port number of an incoming IPv4 packet. In the command line

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			interface, separate the range with a hyphen. For example: 40-90. Note: The destination port can be specified only for TCP and UDP protocols.
destportop	<String>	Read-write	Either the equals (=) or does not equal (!=) logical operator. Possible values = =, !=, EQ, NEQ
destportval	<String>	Read-write	Port number or range of port numbers to match against the destination port number of an incoming IPv4 packet. In the command line interface, separate the range with a hyphen. For example: 40-90. Note: The destination port can be specified only for TCP and UDP protocols. Maximum length = 65535

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
destportdataset	<String>	Read-write	Policy dataset which can have multiple port ranges bound to it.
ttl	<Integer>	Read-write	Number of seconds, in multiples of four, after which the extended ACL rule expires. If you do not want the extended ACL rule to expire, do not specify a TTL value. Minimum value = 1 Maximum value = 2147483647
srcmac	<String>	Read-write	MAC address to match against the source MAC address of an incoming IPv4 packet.
srcmacmask	<String>	Read-write	Used to define range of Source MAC address. It takes string of 0 and 1, 0s are for exact match and 1s for wildcard. For matching first 3 bytes of MAC address, srcMacMask value "000000111111". . Default value: "000000000000"

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
protocol	<String>	Read-write	Protocol to match against the protocol of an incoming IPv4 packet. Possible values = ICMP, IGMP, TCP, EGP, IGP, ARGUS, UDP, RDP, RSVP, EIGRP, L2TP, ISIS, GGP, IPoverIP, ST, CBT, BBN-RCC-M, NVP-II, PUP, EMCON, XNET, CHAOS, MUX, DCN-MEAS, HMP, PRM, XNS-IDP, TRUNK-1, TRUNK-2, LEAF-1, LEAF-2, IRTP, ISO-TP4, NETBLT, MFE-NSP, MERIT-INP, SEP, 3PC, IDPR, XTP, DDP, IDPR-CMTP, TP++, IL, IPv6, SDRP, IPv6-Route, IPv6-Frag, IDRP, GRE, MHRP, BNA, ESP, AH, I-NLSP, SWIPE, NARP, MOBILE, TLSP, SKIP, ICMPV6, IPv6-NoNx, IPv6-Opts, Any-Host-Internal-Protocol, CFTP, Any-Local-

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Network, SAT-EXPAK, KRYPTOLAN, RVD, IPPC, Any-Distributed-File-System, TFTP, VISA, IPCV, CPNX, CPHB, WSN, PVP, BR-SAT-MO, SUN-ND, WB-MON, WB-EXPAK, ISO-IP, VMTP, SECURE-VM, VINES, TTP, NSFNET-IG, DGP, TCF, OSPFIGP, Sprite-RP, LARP, MTP, AX.25, IPIP, MICP, SCC-SP, ETHERIP, Any-Private-Encryption-Scheme, GMTP, IFMP, PNNI, PIM, ARIS, SCPS, QNX, A/N, IPComp, SNP, Compaq-Pe, IPX-in-IP, VRRP, PGM, Any-0-Hop-Protocol, ENCAP, DDX, IATP, STP, SRP, UTI, SMP, SM, PTP, FIRE, CRTP, CRUDP, SSCOPMCE, IPLT, SPS, PIPE, SCTP, FC, RSVP-E2E-

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			IGNORE, Mobility-Header, UDPLite
protocolnumber	<Integer>	Read-write	Protocol to match against the protocol of an incoming IPv4 packet. Minimum value = 1 Maximum value = 255
vlan	<Integer>	Read-write	ID of the VLAN. The Citrix ADC applies the ACL rule only to the incoming packets of the specified VLAN. If you do not specify a VLAN ID, the appliance applies the ACL rule to the incoming packets on all VLANs. Minimum value = 1 Maximum value = 4094
vxlan	<Integer>	Read-write	ID of the VXLAN. The Citrix ADC applies the ACL rule only to the incoming packets of the specified VXLAN. If you do not specify a VXLAN ID, the appliance applies the ACL rule to the incoming packets on all VXLANs.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum value = 1 Maximum value = 16777215
Interface	<String>	Read-write	ID of an interface. The Citrix ADC applies the ACL rule only to the incoming packets from the specified interface. If you do not specify any value, the appliance applies the ACL rule to the incoming packets of all interfaces.
established	<Boolean>	Read-write	Allow only incoming TCP packets that have the ACK or RST bit set, if the action set for the ACL rule is ALLOW and these packets match the other conditions in the ACL rule.
icmptype	<Integer>	Read-write	ICMP Message type to match against the message type of an incoming ICMP packet. For example, to block DESTINATION UNREACHABLE messages, you must specify 3 as the ICMP type.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Note: This parameter can be specified only for the ICMP protocol. Minimum value = 0 Maximum value = 65536
icmpcode	<Integer>	Read-write	Code of a particular ICMP message type to match against the ICMP code of an incoming ICMP packet. For example, to block DESTINATION HOST UNREACHABLE messages, specify 3 as the ICMP type and 1 as the ICMP code. If you set this parameter, you must set the ICMP Type parameter. Minimum value = 0 Maximum value = 65536
priority	<Integer>	Read-write	Priority for the extended ACL rule that determines the order in which it is evaluated relative to the other extended ACL rules. If you do

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			not specify priorities while creating extended ACL rules, the ACL rules are evaluated in the order in which they are created. Minimum value = 1 Maximum value = 100000
state	<String>	Read-write	Enable or disable the extended ACL rule. After you apply the extended ACL rules, the Citrix ADC compares incoming packets against the enabled extended ACL rules. Default value: ENABLED Possible values = ENABLED, DISABLED
logstate	<String>	Read-write	Enable or disable logging of events related to the extended ACL rule. The log messages are stored in the configured syslog or auditlog server. Default value: DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ENABLED, DISABLED
ratelimit	<Integer>	Read-write	Maximum number of log messages to be generated per second. If you set this parameter, you must enable the Log State parameter. Default value: 100 Minimum value = 1 Maximum value = 10000
type	<String>	Read-write	Type of the acl ,default will be CLASSIC. Available options as follows: * CLASSIC - specifies the regular extended acls. * DFD - cluster specific acls,specifies hashmethod for steering of the packet in cluster . Default value: CLASSIC Possible values = CLASSIC, DFD

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
dfdhash	<String>	Read-write	Specifies the type hashmethod to be applied, to steer the packet to the FP of the packet. Possible values = SIP-SPORT-DIP-DPORT, SIP, DIP, SIP-DIP, SIP-SPORT, DIP-DPORT
nodeid	<Integer>	Read-write	Specifies the NodeId to steer the packet to the provided FP. Minimum value = 0 Maximum value = 31
stateful	<String>	Read-write	If stateful option is enabled, transparent sessions are created for the traffic hitting this ACL and not hitting any other features like LB, INAT etc. . Default value: NO Possible values = YES, NO
newname	<String>	Read-write	New name for the extended ACL rule. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Minimum length = 1
hits	<Integer>	Read-only	The hits of this ACL.
kernelstate	<String>	Read-only	The commit status of the ACL. Default value: NOTAPPLIED Possible values = APPLIED, NOTAPPLIED, RE-APPLY, SFAPPLIED, SFNOTAPPLIED, SFAPPLIED61, SFNOTAPPLIED61
aclassociate	<String[]>	Read-only	ACL linked. Possible values = NAT, FORWARDINGSESSION, NAT64, LSN
aclchildcount	<Integer>	Read-only	Number of childs for this ACL.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- ENABLE
- DISABLE
- RENAME
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsacl **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nsacl":{

<b>"aclname":<String_value>,

</b><b>"aclaction":<String_value>,

</b>"td":<Integer_value>,

"srcip":<Boolean_value>,

"srcipop":<String_value>,

"srcipval":<String_value>,

"srcipdataset":<String_value>,

"srcport":<Boolean_value>,

"srcportop":<String_value>,

"srcportval":<String_value>,

"srcportdataset":<String_value>,

"destip":<Boolean_value>,

"destipop":<String_value>,

"destipval":<String_value>,

"destipdataset":<String_value>,
```

```
"destport":<Boolean_value>,

"destportop":<String_value>,

"destportval":<String_value>,

"destportdataset":<String_value>,

"ttl":<Integer_value>,

"srcmac":<String_value>,

"srcmacmask":<String_value>,

"protocol":<String_value>,

"protocolnumber":<Integer_value>,

"vlan":<Integer_value>,

"vxlan":<Integer_value>,

"Interface":<String_value>,

"established":<Boolean_value>,

"icmptype":<Integer_value>,

"icmpcode":<Integer_value>,

"priority":<Integer_value>,

"state":<String_value>,

"logstate":<String_value>,

"ratelimit":<Integer_value>,

"type":<String_value>,

"dfdhash":<String_value>,

"nodeid":<Integer_value>,
```

```
"stateful":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsacl/ aclname_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsacl **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nsacl":{

<b>"aclname":<String_value>,

</b>"aclaction":<String_value>,

"srcip":<Boolean_value>,

"srcipop":<String_value>,
```

```
"srcipval":<String_value>,

"srcport":<Boolean_value>,

"srcportop":<String_value>,

"srcportval":<String_value>,

"destip":<Boolean_value>,

"destipop":<String_value>,

"destipval":<String_value>,

"destport":<Boolean_value>,

"destportop":<String_value>,

"destportval":<String_value>,

"srcmac":<String_value>,

"srcmacmask":<String_value>,

"protocol":<String_value>,

"protocolnumber":<Integer_value>,

"icmptype":<Integer_value>,

"icmpcode":<Integer_value>,

"vlan":<Integer_value>,

"vxlan":<Integer_value>,

"Interface":<String_value>,

"priority":<Integer_value>,

"logstate":<String_value>,

"ratelimit":<Integer_value>,
```

```
"established":<Boolean_value>,

"dfdhash":<String_value>,

"nodeid":<Integer_value>,

"stateful":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsacl? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nsacl":{

<b>"aclname":<String_value>,

</b>"srcip":true,

"srcport":true,

"destip":true,

"destport":true,

"srcmac":true,

"srcmacmask":true,
```

```
"protocol":true,

"icmptype":true,

"icmpcode":true,

"vlan":true,

"vxlan":true,

"Interface":true,

"logstate":true,

"ratelimit":true,

"established":true,

"stateful":true,

"dfdhash":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

ENABLE

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsacl? **action=enable HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nsacl":{

<b>"aclname":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DISABLE

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsacl? **action=disable HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nsacl":{

<b>"aclname":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

RENAME

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsacl? **action=rename HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nsacl":{

<b>"aclname":<String_value>,

</b><b>"newname":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsacl **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/nsacl? **args=aclname: <String_value> ,type: <String_value>**

Use this query-parameter to get nsacl resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/config/nsacl? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/nsacl? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of nsacl resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/nsacl? **view=summary**

Use this query-parameter to get the summary output of nsacl resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/nsacl? **pagesize=#no;pageno=#no**

Use this query-parameter to get the nsacl resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nsacl": [ {

aclname:<String_value>,type:<String_value>"td":<Integer_value>,

"aclaction":<String_value>,

"srcmac":<String_value>,

"srcmacmask":<String_value>,

"protocol":<String_value>,

"protocolnumber":<Integer_value>,

"srcportval":<String_value>,

"srcportdataset":<String_value>,

"srcportop":<String_value>,

"destportval":<String_value>,

"destportdataset":<String_value>,

"destportop":<String_value>,

"srcipval":<String_value>,
```

```
"srcipdataset":<String_value>,

"srcipop":<String_value>,

"destipval":<String_value>,

"destipop":<String_value>,

"destipdataset":<String_value>,

"vlan":<Integer_value>,

"vxlan":<Integer_value>,

"state":<String_value>,

"ttl":<Integer_value>,

"icmptype":<Integer_value>,

"icmpcode":<Integer_value>,

"Interface":<String_value>,

"hits":<Integer_value>,

"established":<Boolean_value>,

"priority":<Integer_value>,

"kernelstate":<String_value>,

"logstate":<String_value>,

"ratelimit":<Integer_value>,

"aclassociate":<String[]_value>,

"dfdhash":<String_value>,

"nodeid":<Integer_value>,

"stateful":<String_value>,
```

```
"aclchildcount":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsacl/ aclname_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/nsacl/ aclname_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/nsacl/ aclname_value<String> ? **view=summary**

Use this query-parameter to get the summary output of nsacl resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "nsacl": [ {

aclname:<String_value>,type:<String_value>"td":<Integer_value>,
```

```
"aclaction":<String_value>,

"srcmac":<String_value>,

"srcmacmask":<String_value>,

"protocol":<String_value>,

"protocolnumber":<Integer_value>,

"srcportval":<String_value>,

"srcportdataset":<String_value>,

"srcportop":<String_value>,

"destportval":<String_value>,

"destportdataset":<String_value>,

"destportop":<String_value>,

"srcipval":<String_value>,

"srcipdataset":<String_value>,

"srcipop":<String_value>,

"destipval":<String_value>,

"destipop":<String_value>,

"destipdataset":<String_value>,

"vlan":<Integer_value>,

"vxlan":<Integer_value>,

"state":<String_value>,

"ttl":<Integer_value>,

"icmptype":<Integer_value>,
```

```
"icmpcode":<Integer_value>,

"Interface":<String_value>,

"hits":<Integer_value>,

"established":<Boolean_value>,

"priority":<Integer_value>,

"kernelstate":<String_value>,

"logstate":<String_value>,

"ratelimit":<Integer_value>,

"aclassociate":<String[]_value>,

"dfdhash":<String_value>,

"nodeid":<Integer_value>,

"stateful":<String_value>,

"aclchildcount":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsacl? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nsacl": [ { "__count": "#no"} ] }
```

nsacl6

Configuration for ACL6 entry resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
acl6name	<String>	Read-write	Name for the ACL6 rule. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Minimum length = 1
acl6action	<String>	Read-write	Action to perform on the incoming IPv6 packets that match the ACL6 rule.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Available settings function as follows: * ALLOW - The Citrix ADC processes the packet. * BRIDGE - The Citrix ADC bridges the packet to the destination without processing it. * DENY - The Citrix ADC drops the packet. Possible values = BRIDGE, DENY, ALLOW
td	<Integer>	Read-write	Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0. Minimum value = 0 Maximum value = 4094
srcipv6	<Boolean>	Read-write	IP address or range of IP addresses to

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			match against the source IP address of an incoming IPv6 packet. In the command line interface, separate the range with a hyphen.
srcipop	<String>	Read-write	Either the equals (=) or does not equal (!=) logical operator. Possible values = =, !=, EQ, NEQ
srcipv6val	<String>	Read-write	Source IPv6 address (range).
srcport	<Boolean>	Read-write	Port number or range of port numbers to match against the source port number of an incoming IPv6 packet. In the command line interface, separate the range with a hyphen. For example: 40-90. Note: The destination port can be specified only for TCP and UDP protocols.
srcportop	<String>	Read-write	Either the equals (=) or does not equal (!=) logical operator.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = =, !=, EQ, NEQ
srcportval	<String>	Read-write	Source port (range). Maximum length = 65535
destipv6	<Boolean>	Read-write	IP address or range of IP addresses to match against the destination IP address of an incoming IPv6 packet. In the command line interface, separate the range with a hyphen.
destipop	<String>	Read-write	Either the equals (=) or does not equal (!=) logical operator. Possible values = =, !=, EQ, NEQ
destipv6val	<String>	Read-write	Destination IPv6 address (range).
destport	<Boolean>	Read-write	Port number or range of port numbers to match against the destination port number of an incoming IPv6 packet. In the command line interface, separate the range with a

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			hyphen. For example: 40-90. Note: The destination port can be specified only for TCP and UDP protocols.
destportop	<String>	Read-write	Either the equals (=) or does not equal (!=) logical operator. Possible values = =, !=, EQ, NEQ
destportval	<String>	Read-write	Destination port (range). Maximum length = 65535
ttl	<Integer>	Read-write	Time to expire this ACL6 (in seconds). Minimum value = 1 Maximum value = 2147483647
srcmac	<String>	Read-write	MAC address to match against the source MAC address of an incoming IPv6 packet.
srcmacmask	<String>	Read-write	Used to define range of Source MAC address. It takes string of 0 and 1, 0s are for exact match and 1s for wildcard. For matching first 3 bytes of MAC

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			address, srcMacMask value "000000111111". . Default value: "000000000000"
protocol	<String>	Read-write	Protocol, identified by protocol name, to match against the protocol of an incoming IPv6 packet. Possible values = ICMPV6, TCP, UDP, ICMP, IGMP, EGP, IGP, ARGUS, RDP, RSVP, EIGRP, L2TP, ISIS, GGP, IPoverIP, ST, CBT, BBN-RCC-M, NVP-II, PUP, EMCON, XNET, CHAOS, MUX, DCN-MEAS, HMP, PRM, XNS-IDP, TRUNK-1, TRUNK-2, LEAF-1, LEAF-2, IRTP, ISO-TP4, NETBLT, MFE-NSP, MERIT-INP, SEP, 3PC, IDPR, XTP, DDP, IDPR-CMTP, TP++, IL, IPv6, SDRP, IPv6-Route, IPv6-Frag, IDRP, GRE, MHRP, BNA, ESP, AH, I-NLSP,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			SWIPE, NARP, MOBILE, TLSP, SKIP, IPv6-NoNx, IPv6-Opts, Any-Host-Internal-Protocol, CFTP, Any-Local-Network, SAT-EXPAK, KRYPTOLAN, RVD, IPPC, Any-Distributed-File-System, TFTP, VISA, IPCV, CPNX, CPHB, WSN, PVP, BR-SAT-MO, SUN-ND, WB-MON, WB-EXPAK, ISO-IP, VMTP, SECURE-VM, VINES, TTP, NSFNET-IG, DGP, TCF, OSPFIGP, Sprite-RP, LARP, MTP, AX.25, IPIP, MICP, SCC-SP, ETHERIP, Any-Private-Encryption-Scheme, GMTP, IFMP, PNNI, PIM, ARIS, SCPS, QNX, A/N, IPComp, SNP, Compaq-Pe, IPX-in-IP, VRRP, PGM, Any-0-Hop-Protocol, ENCAP, DDX, IATP, STP, SRP, UTI, SMP, SM,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			PTP, FIRE, CRTP, CRUDP, SSCOPMCE, IPLT, SPS, PIPE, SCTP, FC, RSVP-E2E-IGNORE, Mobility-Header, UDPLite
protocolnumber	<Integer>	Read-write	Protocol, identified by protocol number, to match against the protocol of an incoming IPv6 packet. Minimum value = 1 Maximum value = 255
vlan	<Integer>	Read-write	ID of the VLAN. The Citrix ADC applies the ACL6 rule only to the incoming packets on the specified VLAN. If you do not specify a VLAN ID, the appliance applies the ACL6 rule to the incoming packets on all VLANs. Minimum value = 1 Maximum value = 4094
vxlan	<Integer>	Read-write	ID of the VXLAN. The Citrix ADC applies the ACL6 rule only to the incoming packets on

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			the specified VXLAN. If you do not specify a VXLAN ID, the appliance applies the ACL6 rule to the incoming packets on all VXLANs. Minimum value = 1 Maximum value = 16777215
Interface	<String>	Read-write	ID of an interface. The Citrix ADC applies the ACL6 rule only to the incoming packets from the specified interface. If you do not specify any value, the appliance applies the ACL6 rule to the incoming packets from all interfaces.
established	<Boolean>	Read-write	Allow only incoming TCP packets that have the ACK or RST bit set if the action set for the ACL6 rule is ALLOW and these packets match the other conditions in the ACL6 rule.
icmptype	<Integer>	Read-write	ICMP Message type to match against the message type of an incoming IPv6 ICMP

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			packet. For example, to block DESTINATION UNREACHABLE messages, you must specify 3 as the ICMP type. Note: This parameter can be specified only for the ICMP protocol. Minimum value = 0 Maximum value = 65536
icmpcode	<Integer>	Read-write	Code of a particular ICMP message type to match against the ICMP code of an incoming IPv6 ICMP packet. For example, to block DESTINATION HOST UNREACHABLE messages, specify 3 as the ICMP type and 1 as the ICMP code. If you set this parameter, you must set the ICMP Type parameter. Minimum value = 0 Maximum value = 65536

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
priority	<Integer>	Read-write	Priority for the ACL6 rule, which determines the order in which it is evaluated relative to the other ACL6 rules. If you do not specify priorities while creating ACL6 rules, the ACL6 rules are evaluated in the order in which they are created. Minimum value = 1 Maximum value = 81920
state	<String>	Read-write	State of the ACL6. Default value: ENABLED Possible values = ENABLED, DISABLED
type	<String>	Read-write	Type of the acl6 ,default will be CLASSIC. Available options as follows: * CLASSIC - specifies the regular extended acls. * DFD - cluster specific acls,specifies hashmethod for

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			steering of the packet in cluster . Default value: CLASSIC Possible values = CLASSIC, DFD
dfdhash	<String>	Read-write	Specifies the type of hashmethod to be applied, to steer the packet to the FP of the packet. Possible values = SIP-SPORT-DIP-DPORT, SIP, DIP, SIP-DIP, SIP-SPORT, DIP-DPORT
dfdprefix	<Integer>	Read-write	hashprefix to be applied to SIP/DIP to generate rsshash FP.eg 128 => hash calculated on the complete IP. Default value: 128 Minimum value = 1 Maximum value = 128
nodeid	<Integer>	Read-write	Specifies the NodeId to steer the packet to the provided FP. Minimum value = 0

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum value = 31
stateful	<String>	Read-write	If stateful option is enabled, transparent sessions are created for the traffic hitting this ACL6 and not hitting any other features like LB, INAT etc. . Default value: NO Possible values = YES, NO
logstate	<String>	Read-write	Enable or disable logging of events related to the ACL6 rule. The log messages are stored in the configured syslog or auditlog server. Default value: DISABLED Possible values = ENABLED, DISABLED
ratelimit	<Integer>	Read-write	Maximum number of log messages to be generated per second. If you set this parameter, you must enable the Log State parameter. Default value: 100

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum value = 1 Maximum value = 10000
aclaction	<String>	Read-write	Action associated with the ACL6. Possible values = BRIDGE, DENY, ALLOW
newname	<String>	Read-write	New name for the ACL6 rule. Must begin with an ASCII alphabetic or underscore \(_\) character, and must contain only ASCII alphanumeric, underscore, hash \(#\), period \(.\), space, colon \(:\), at \(@\), equals \(=\), and hyphen \(-\) characters. Minimum length = 1
kernelstate	<String>	Read-only	Commit status of the ACL6. Default value: NOTAPPLIED Possible values = APPLIED, NOTAPPLIED, RE-APPLY, SFAPPLIED, SFNOTAPPLIED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
hits	<Integer>	Read-only	Number of hits of this ACL6.
aclassociate	<String[]>	Read-only	ACL6 linked. Possible values = NAT, FORWARDINGSESSION, NAT64, LSN
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- ENABLE
- DISABLE
- RENAME
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsacl6 **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nsacl6":{

<b>"acl6name":<String_value>,

</b><b>"acl6action":<String_value>,

</b>"td":<Integer_value>,

"srcipv6":<Boolean_value>,

"srcipop":<String_value>,

"srcipv6val":<String_value>,
```

```
"srcport":<Boolean_value>,

"srcportop":<String_value>,

"srcportval":<String_value>,

"destipv6":<Boolean_value>,

"destipop":<String_value>,

"destipv6val":<String_value>,

"destport":<Boolean_value>,

"destportop":<String_value>,

"destportval":<String_value>,

"ttl":<Integer_value>,

"srcmac":<String_value>,

"srcmacmask":<String_value>,

"protocol":<String_value>,

"protocolnumber":<Integer_value>,

"vlan":<Integer_value>,

"vxlan":<Integer_value>,

"Interface":<String_value>,

"established":<Boolean_value>,

"icmptype":<Integer_value>,

"icmpcode":<Integer_value>,

"priority":<Integer_value>,

"state":<String_value>,
```

```
"type":<String_value>,

"dfdhash":<String_value>,

"dfdprefix":<Integer_value>,

"nodeid":<Integer_value>,

"stateful":<String_value>,

"logstate":<String_value>,

"ratelimit":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsacl6/ acl6name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsacl6 **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nsacl6":{

<b>"acl6name":<String_value>,

</b>"aclaction":<String_value>,

"srcipv6":<Boolean_value>,

"srcipop":<String_value>,

"srcipv6val":<String_value>,

"srcport":<Boolean_value>,

"srcportop":<String_value>,

"srcportval":<String_value>,

"destipv6":<Boolean_value>,

"destipop":<String_value>,

"destipv6val":<String_value>,

"destport":<Boolean_value>,

"destportop":<String_value>,

"destportval":<String_value>,

"srcmac":<String_value>,

"srcmacmask":<String_value>,

"protocol":<String_value>,

"protocolnumber":<Integer_value>,

"icmptype":<Integer_value>,

"icmpcode":<Integer_value>,
```

```
"vlan":<Integer_value>,

"vxlan":<Integer_value>,

"Interface":<String_value>,

"priority":<Integer_value>,

"logstate":<String_value>,

"ratelimit":<Integer_value>,

"established":<Boolean_value>,

"dfdhash":<String_value>,

"dfdprefix":<Integer_value>,

"nodeid":<Integer_value>,

"stateful":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsacl6? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nsacl6":{

<b>"acl6name":<String_value>,

</b>"srcipv6":true,

"srcport":true,

"destipv6":true,

"destport":true,

"srcmac":true,

"srcmacmask":true,

"protocol":true,

"icmptype":true,

"icmpcode":true,

"vlan":true,

"vxlan":true,

"Interface":true,

"logstate":true,

"ratelimit":true,

"established":true,

"stateful":true,

"dfdhash":true,

"dfdprefix":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

ENABLE

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsacl6? **action=enable HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nsacl6":{

<b>"acl6name":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DISABLE

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsacl6? **action=disable HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nsacl6":{

<b>"acl6name":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

RENAME

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsacl6? **action=rename HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nsacl6":{

<b>"acl6name":<String_value>,

</b><b>"newname":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsacl6 **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/nsacl6? **args=acl6name: <String_value> ,type: <String_value>**

Use this query-parameter to get nsacl6 resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/config/nsacl6? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/nsacl6? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of nsacl6 resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/nsacl6? **view=summary**

Use this query-parameter to get the summary output of nsacl6 resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/nsacl6? **pagesize=#no;pageno=#no**

Use this query-parameter to get the nsacl6 resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nsacl6": [ {

acl6name:<String_value>,type:<String_value>"acl6action":<String_value>,

"srcmac":<String_value>,

"srcmacmask":<String_value>,

"protocol":<String_value>,
```

```
"protocolnumber":<Integer_value>,

"srcportval":<String_value>,

"srcportop":<String_value>,

"destportval":<String_value>,

"destportop":<String_value>,

"srcipv6val":<String_value>,

"srcipop":<String_value>,

"destipv6val":<String_value>,

"destipop":<String_value>,

"vlan":<Integer_value>,

"vxlan":<Integer_value>,

"state":<String_value>,

"kernelstate":<String_value>,

"ttl":<Integer_value>,

"icmptype":<Integer_value>,

"icmpcode":<Integer_value>,

"Interface":<String_value>,

"hits":<Integer_value>,

"established":<Boolean_value>,

"priority":<Integer_value>,

"logstate":<String_value>,

"ratelimit":<Integer_value>,
```

```
"td":<Integer_value>,

"aclassociate":<String[]_value>,

"dfdhash":<String_value>,

"dfdprefix":<Integer_value>,

"nodeid":<Integer_value>,

"stateful":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsacl6/ acl6name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/nsacl6/ acl6name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/nsacl6/ acl6name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of nsacl6 resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "nsacl6": [ {

acl6name:<String_value>,type:<String_value>"acl6action":<String_value>,

"srcmac":<String_value>,

"srcmacmask":<String_value>,

"protocol":<String_value>,

"protocolnumber":<Integer_value>,

"srcportval":<String_value>,

"srcportop":<String_value>,

"destportval":<String_value>,

"destportop":<String_value>,

"srcipv6val":<String_value>,

"srcipop":<String_value>,

"destipv6val":<String_value>,

"destipop":<String_value>,

"vlan":<Integer_value>,

"vxlan":<Integer_value>,

"state":<String_value>,

"kernelstate":<String_value>,

"ttl":<Integer_value>,
```

```
"icmptype":<Integer_value>,

"icmpcode":<Integer_value>,

"Interface":<String_value>,

"hits":<Integer_value>,

"established":<Boolean_value>,

"priority":<Integer_value>,

"logstate":<String_value>,

"ratelimit":<Integer_value>,

"td":<Integer_value>,

"aclassociate":<String[]_value>,

"dfdhash":<String_value>,

"dfdprefix":<Integer_value>,

"nodeid":<Integer_value>,

"stateful":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsacl6? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nsacl6": [ { "__count": "#no"} ] }
```

nsacls

Configuration for ACL entry resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
type	<String>	Read-write	Type of the acl ,default will be CLASSIC. Available options as follows: * CLASSIC - specifies the regular extended acls. * DFD - cluster specific acls,specifies hashmethod for steering of the packet in cluster . Default value: CLASSIC

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = CLASSIC, DFD

Operations

(click to see Properties)

- RENUMBER
- CLEAR
- APPLY

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

RENUMBER

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsacls? **action=renumber HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nsacls":{

"type":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

CLEAR

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsacls? **action=clear HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nsacls":{

"type":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

APPLY

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsacls? **action=apply HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nsacls":{

"type":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

nsacls6

Configuration for ACL6 entry resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
type	<String>	Read-write	Type of the acl ,default will be CLASSIC. Available options as follows:

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			* CLASSIC - specifies the regular extended acls. * DFD - cluster specific acls,specifies hashmethod for steering of the packet in cluster . Default value: CLASSIC Possible values = CLASSIC, DFD

Operations

(click to see Properties)

- CLEAR
- APPLY
- RENUMBER

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

CLEAR

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsacls6? **action=clear HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nsacls6":{

"type":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

APPLY

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsacls6? **action=apply HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nsacls6":{

"type":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

RENUMBER

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsacls6? **action=renumber HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nsacls6":{

"type":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

nsappflowcollector

Configuration for appflowCollector resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the AppFlow collector. Minimum length = 1 Maximum length = 127
ipaddress	<String>	Read-write	The IPv4 address of the AppFlow collector.
port	<Integer>	Read-write	The UDP port on which the AppFlow collector is listening. Default value: 4739
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsappflowcollector **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nsappflowcollector":{

<b>"name":<String_value>,

</b><b>"ipaddress":<String_value>,

</b>"port":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsappflowcollector/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsappflowcollector **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/nsappflowcollector? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/nsappflowcollector? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of nsappflowcollector resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/nsappflowcollector? **view=summary**

Use this query-parameter to get the summary output of nsappflowcollector resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/nsappflowcollector? **pagesize=#no;pageno=#no**

Use this query-parameter to get the nsappflowcollector resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nsappflowcollector": [ {

"name":<String_value>,

"ipaddress":<String_value>,

"port":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsappflowcollector/ name_value<String>
Query-parameters: attrs http:// <netscaler-ip-address> /nitro/v1/config/nsappflowcollector/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/nsappflowcollector/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of nsappflowcollector resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "nsappflowcollector": [ {

"name":<String_value>,

"ipaddress":<String_value>,

"port":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsappflowcollector? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nsappflowcollector": [ { "__count": "#no"} ] }
```

nsappflowparam

Configuration for appflowParam resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
templaterefresh	<Integer>	Read-write	IPFIX template refresh interval (in seconds). Default value: 600 Minimum value = 60 Maximum value = 3600
udppmtu	<Integer>	Read-write	MTU to be used for IPFIX UDP packets. Default value: 1472 Minimum value = 128 Maximum value = 1472

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
httpurl	<String>	Read-write	Enable AppFlow HTTP URL logging. Default value: DISABLED Possible values = ENABLED, DISABLED
httpcookie	<String>	Read-write	Enable AppFlow HTTP cookie logging. Default value: DISABLED Possible values = ENABLED, DISABLED
httpreferer	<String>	Read-write	Enable AppFlow HTTP referer logging. Default value: DISABLED Possible values = ENABLED, DISABLED
httpmethod	<String>	Read-write	Enable AppFlow HTTP method logging. Default value: DISABLED Possible values = ENABLED, DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
httphost	<String>	Read-write	Enable AppFlow HTTP host logging. Default value: DISABLED Possible values = ENABLED, DISABLED
httpuseragent	<String>	Read-write	Enable AppFlow HTTP user-agent logging. Default value: DISABLED Possible values = ENABLED, DISABLED
clienttrafficonly	<String>	Read-write	Control whether AppFlow records should be generated only for client-side traffic. Default value: NO Possible values = YES, NO
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- UPDATE
- UNSET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsappflowparam **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nsappflowparam":{

"templaterefresh":<Integer_value>,

"udppmtu":<Integer_value>,

"httpurl":<String_value>,
```

```
"httpcookie":<String_value>,

"httpreferer":<String_value>,

"httpmethod":<String_value>,

"httphost":<String_value>,

"httpuseragent":<String_value>,

"clienttrafficonly":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsappflowparam? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nsappflowparam":{

"templaterefresh":true,

"udppmtu":true,

"httpurl":true,

"httpcookie":true,
```

```
"httpreferer":true,

"httpmethod":true,

"httphost":true,

"httpuseragent":true,

"clienttrafficonly":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsappflowparam **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nsappflowparam": [ {

"templaterefresh":<Integer_value>,

"udppmtu":<Integer_value>,
```

```
"httpurl":<String_value>,

"httpcookie":<String_value>,

"httpreferer":<String_value>,

"httpmethod":<String_value>,

"httphost":<String_value>,

"httpuseragent":<String_value>,

"clienttrafficonly":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

nsaptlicense

Configuration for aptlicense resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
serialno	<String>	Read-write	Hardware Serial Number/License Activation Code(LAC).
useproxy	<String>	Read-write	Specifies whether to use the licenseproxyserver to reach the internet. Make sure to configure licenseproxyserver to use this option.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: NO Possible values = YES, NO
id	<String>	Read-write	License ID.
sessionid	<String>	Read-write	Session ID.
bindtype	<String>	Read-write	Bind type.
countavailable	<String>	Read-write	The user can allocate one or more licenses. Ensure the value is less than (for partial allocation) or equal to the total number of available licenses.
licensedir	<String>	Read-write	License Directory.
response	<String>	Read-only	Response data as text blob.
counttotal	<String>	Read-only	Count.
name	<String>	Read-only	License name.
relevance	<String>	Read-only	License relevance.
datepurchased	<String>	Read-only	License purchase date.
datesa	<String>	Read-only	License SA date.
dateexp	<String>	Read-only	License expiry date.
features	<String[]>	Read-only	Features.
_nextgenapiresource	<String>	Read-only	.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET (ALL)
- COUNT
- CHANGE

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

CHANGE

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsaptlicense? **action=update HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nsaptlicense":{

<b>"id":<String_value>,

</b><b>"sessionid":<String_value>,

</b><b>"bindtype":<String_value>,

</b><b>"countavailable":<String_value>,

</b>"licensedir":<String_value>,

"useproxy":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsaptlicense **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/nsaptlicense? **args= serialno:<String_value>, useproxy: <String_value>**

Use this query-parameter to get nsaptlicense resources based on additional properties.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nsaptlicense": [ {

<b>serialno:<String_value>,</
b>useproxy:<String_value>"response":<String_value>,

"id":<String_value>,

"sessionid":<String_value>,

"bindtype":<String_value>,

"countavailable":<String_value>,

"counttotal":<String_value>,

"name":<String_value>,

"relevance":<String_value>,

"datepurchased":<String_value>,

"datesa":<String_value>,

"dateexp":<String_value>,

"features":<String[]_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsaptlicense? **args= serialno:<String_value>, useproxy: <String_value> ;count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nsaptlicense": [ { "__count": "#no"} ] }
```

nsassignment

Configuration for assignment resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the assignment. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space ( ),

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			at (@), equals (=), colon (:), and underscore characters. Can be changed after the assignment is added. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my assignment" or my assignment).
variable	<String>	Read-write	Left hand side of the assigment, of the form $variable-name (for a singleton variabled) or $variable-name[key-expression], where key-expression is an expression that evaluates to a text string and provides the key to select a map entry.
set	<String>	Read-write	Right hand side of the assignment. The expression is evaluated and

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			assigned to the left hand variable.
Add	<String>	Read-write	Right hand side of the assignment. The expression is evaluated and added to the left hand variable.
sub	<String>	Read-write	Right hand side of the assignment. The expression is evaluated and subtracted from the left hand variable.
append	<String>	Read-write	Right hand side of the assignment. The expression is evaluated and appended to the left hand variable.
clear	<Boolean>	Read-write	Clear the variable value. Deallocates a text value, and for a map, the text key.
comment	<String>	Read-write	Comment. Can be used to preserve information about this rewrite action.
newname	<String>	Read-write	New name for the assignment. Must begin with a letter, number, or the underscore character (_), and must contain only

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			letters, numbers, and the hyphen (-), period (.) hash (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Can be changed after the rewrite policy is added. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my assignment" or my assignment). Minimum length = 1
hits	<Integer>	Read-only	The number of times the action has been taken.
undefhits	<Integer>	Read-only	The number of times the action resulted in UNDEF.
referencecount	<Integer>	Read-only	The number of references to the action.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- UPDATE
- UNSET
- DELETE
- GET (ALL)
- GET
- COUNT
- RENAME

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsassignment **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nsassignment":{

<b>"name":<String_value>,

</b><b>"variable":<String_value>,

</b>"set":<String_value>,

"Add":<String_value>,

"sub":<String_value>,

"append":<String_value>,

"clear":<Boolean_value>,

"comment":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsassignment **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nsassignment":{

<b>"name":<String_value>,

</b>"variable":<String_value>,

"set":<String_value>,

"Add":<String_value>,

"sub":<String_value>,

"append":<String_value>,

"clear":<Boolean_value>,

"comment":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsassignment? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nsassignment":{

<b>"name":<String_value>,

</b>"comment":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsassignment/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

RENAME

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsassignment? **action=rename HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nsassignment":{

<b>"name":<String_value>,

</b><b>"newname":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsassignment **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/nsassignment? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/nsassignment? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of nsassignment resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/nsassignment? **view=summary**

Use this query-parameter to get the summary output of nsassignment resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/nsassignment? **pagesize=#no;pageno=#no**

Use this query-parameter to get the nsassignment resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nsassignment": [ {

"name":<String_value>,

"variable":<String_value>,

"set":<String_value>,

"Add":<String_value>,

"sub":<String_value>,

"append":<String_value>,

"clear":<Boolean_value>,

"hits":<Integer_value>,

"undefhits":<Integer_value>,

"referencecount":<Integer_value>,

"comment":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsassignment/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/nsassignment/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/nsassignment/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of nsassignment resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "nsassignment": [ {

"name":<String_value>,

"variable":<String_value>,

"set":<String_value>,

"Add":<String_value>,
```

```
"sub":<String_value>,

"append":<String_value>,

"clear":<Boolean_value>,

"hits":<Integer_value>,

"undefhits":<Integer_value>,

"referencecount":<Integer_value>,

"comment":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsassignment? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nsassignment": [ { "__count": "#no"} ] }
```

nscapacity

Configuration for capacity resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
bandwidth	<Integer>	Read-write	System bandwidth limit.
platform	<String>	Read-write	appliance platform type. Possible values = VS10, VE10, VP10, VS25, VE25, VP25, VS50, VE50, VP50, VS200, VE200, VP200, VS1000, VE1000, VP1000, VS3000, VE3000, VP3000, VS5000, VE5000, VP5000, VS8000, VE8000, VP8000, VS10000, VE10000, VP10000, VS15000, VE15000, VP15000, VS25000, VE25000, VP25000, VS40000, VE40000, VP40000, VS100000,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			VE100000, VP100000, CP1000
vcpu	<Boolean>	Read-write	licensed using vcpu pool.
edition	<String>	Read-write	Product edition. Possible values = Standard, Enterprise, Platinum
unit	<String>	Read-write	Bandwidth unit. Possible values = Gbps, Mbps
username	<String>	Read-write	Username to authenticate with ADM Agent for LAS licensing. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Minimum length = 1 Maximum length = 127
password	<String>	Read-write	Password to use when authenticating with ADM Agent for LAS licensing. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ignoreexpiry	<Boolean>	Read-write	Value to mention if days to expire data needs to be fetched or not. Default value: 0
nodeid	<Integer>	Read-write	Unique number that identifies the cluster node. Minimum value = 0 Maximum value = 31
actualbandwidth	<Integer>	Read-only	Bandwith in MBPS.
vcpucount	<Integer>	Read-only	number of vCPUs licensed. Minimum value = 1 Maximum value = 20
maxvcpucount	<Integer>	Read-only	number of max vCPUs. Minimum value = 1 Maximum value = 20
maxbandwidth	<Integer>	Read-only	Maximum Bandwidth.
minbandwidth	<Integer>	Read-only	Minimum Bandwidth.
instancecount	<Integer>	Read-only	VPX will consume one instance and MPX will consume zero instance.
daystoexpiration	<Integer>	Read-only	Days to expire.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum value = 0 Maximum value = 4294967294
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- UPDATE
- UNSET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/nscapacity **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nscapacity":{

"bandwidth":<Integer_value>,

"platform":<String_value>,

"vcpu":<Boolean_value>,

"edition":<String_value>,

"unit":<String_value>,

"username":<String_value>,

"password":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/nscapacity? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nscapacity":{

"bandwidth":true,

"platform":true,

"vcpu":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/nscapacity **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/nscapacity? **args=ignoreexpiry: <Boolean_value> ,nodeid: <Integer_value>**

Use this query-parameter to get nscapacity resources based on additional properties.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nscapacity": [ {

ignoreexpiry:<Boolean_value>,nodeid:<Integer_value>"actualbandwidth":<Integer_value>,

"platform":<String_value>,

"vcpucount":<Integer_value>,

"maxvcpucount":<Integer_value>,

"edition":<String_value>,

"unit":<String_value>,

"bandwidth":<Integer_value>,

"maxbandwidth":<Integer_value>,

"minbandwidth":<Integer_value>,

"instancecount":<Integer_value>,

"daystoexpiration":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

nscentralmanagementserver

Configuration for centralmanagementserver resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
type	<String>	Read-write	Type of the central management server. Must be either CLOUD or ONPREM depending on whether the server is on the cloud or on premise. Possible values = CLOUD, ONPREM
username	<String>	Read-write	Username for access to central management server. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my ns

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			centralmgmtserver" or "my ns centralmgmtserver") . Minimum length = 1 Maximum length = 127
password	<String>	Read-write	Password for access to central management server. Required for any user account. Minimum length = 1 Maximum length = 127
activationcode	<String>	Read-write	Activation code is used to register to ADM service. Minimum length = 1 Maximum length = 127
ipaddress	<String>	Read-write	Ip Address of central management server. Minimum length = 1
servername	<String>	Read-write	Fully qualified domain name of the central management server or service-url to locate ADM service.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
validatecert	<String>	Read-write	validate the server certificate for secure SSL connections. Default value: YES Possible values = YES, NO
deviceprofilename	<String>	Read-write	Device profile is created on ADM and contains the user name and password of the instance(s). Minimum length = 1 Maximum length = 255
adcusername	<String>	Read-write	ADC username used to create device profile on ADM. Minimum length = 1 Maximum length = 127
adcpassword	<String>	Read-write	ADC password used to create device profile on ADM. Minimum length = 1 Maximum length = 127
instanceid	<String>	Read-only	Instance ID of the customer provided by Trust.
customerid	<String>	Read-only	Customer ID of the citrix cloud customer.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
admserviceenvironment	<String>	Read-only	ADM service environment (PRODUCTION/STAGING/DEV). Possible values = PRODUCTION, STAGING, DEV
admserviceconnectionstatus	<String>	Read-only	Built-in agent's (mastools) connection status to ADM service. Possible values = CONNECTED, DISCONNECTED
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/nscentralmanagementserver **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nscentralmanagementserver":{

<b>"type":<String_value>,

</b>"username":<String_value>,

"password":<String_value>,

"activationcode":<String_value>,

"ipaddress":<String_value>,
```

```
"servername":<String_value>,

"validatecert":<String_value>,

"deviceprofilename":<String_value>,

"adcusername":<String_value>,

"adcpassword":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/nscentralmanagementserver/ type_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/nscentralmanagementserver **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/nscentralmanagementserver? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/nscentralmanagementserver? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of nscentralmanagementserver resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/nscentralmanagementserver? **view=summary**

Use this query-parameter to get the summary output of nscentralmanagementserver resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/nscentralmanagementserver? **pagesize=#no;pageno=#no**

Use this query-parameter to get the nscentralmanagementserver resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nscentralmanagementserver": [ {

"type":<String_value>,

"username":<String_value>,

"ipaddress":<String_value>,

"servername":<String_value>,

"validatecert":<String_value>,
```

```
"password":<String_value>,

"deviceprofilename":<String_value>,

"instanceid":<String_value>,

"customerid":<String_value>,

"admserviceenvironment":<String_value>,

"admserviceconnectionstatus":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/nscentralmanagementserver/ type_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/ nscentralmanagementserver/ type_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/nscentralmanagementserver/ type_value<String> ? **view=summary**

Use this query-parameter to get the summary output of nscentralmanagementserver resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "nscentralmanagementserver": [ {

"type":<String_value>,

"username":<String_value>,

"ipaddress":<String_value>,

"servername":<String_value>,

"validatecert":<String_value>,

"password":<String_value>,

"deviceprofilename":<String_value>,

"instanceid":<String_value>,

"customerid":<String_value>,

"admserviceenvironment":<String_value>,

"admserviceconnectionstatus":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/nscentralmanagementserver? **count=yes**
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nscentralmanagementserver": [ { "__count": "#no"} ] }
```

nschannelparam

Configuration for 0 resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
vfautorecover	<String>	Read-write	VF autorecover mode. Default value: ENABLE Possible values = DISABLE, ENABLE
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- UPDATE
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/nschannelparam **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nschannelparam":{

<b>"vfautorecover":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/nschannelparam **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nschannelparam": [ {

"vfautorecover":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

nsconfig

Configuration for system config resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
force	<Boolean>	Read-write	Configurations will be cleared without prompting for confirmation.
level	<String>	Read-write	Types of configurations to be cleared. * basic: Clears all configurations except the following: - NSIP, default route (gateway), static routes, MIPs, and SNIPs - Network settings (DG, VLAN, RHI and DNS settings) - Cluster settings - HA node definitions - Feature and mode settings - nsroot password * extended: Clears the same configurations as the 'basic' option. In addition, it clears

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			the feature and mode settings. * full: Clears all configurations except NSIP, default route, and interface settings. Note: When you clear the configurations through the cluster IP address, by specifying the level as 'full', the cluster is deleted and all cluster nodes become standalone appliances. The 'basic' and 'extended' levels are propagated to the cluster nodes. Possible values = basic, extended, full
rbaconfig	<String>	Read-write	RBA configurations and TACACS policies bound to system global will not be cleared if RBA is set to NO.This option is applicable only for BASIC level of clear configuration.Default is YES, which will

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			clear rba configurations. Default value: YES Possible values = YES, NO
ipaddress	<String>	Read-write	IP address of the Citrix ADC. Commonly referred to as NSIP address. This parameter is mandatory to bring up the appliance. Minimum length = 1
netmask	<String>	Read-write	Netmask corresponding to the IP address. This parameter is mandatory to bring up the appliance.
nsvlan	<Integer>	Read-write	VLAN (NSVLAN) for the subnet on which the IP address resides. Minimum value = 2 Maximum value = 4094
ifnum	<String[]>	Read-write	Interfaces of the appliances that must be bound to the NSVLAN. Minimum length = 1
tagged	<String>	Read-write	Specifies that the interfaces will be added as 802.1q

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			tagged interfaces. Packets sent on these interface on this VLAN will have an additional 4-byte 802.1q tag which identifies the VLAN. To use 802.1q tagging, the switch connected to the appliance's interfaces must also be configured for tagging. Default value: YES Possible values = YES, NO
httpport	<Integer[]>	Read-write	The HTTP ports on the Web server. This allows the system to perform connection off-load for any client request that has a destination port matching one of these configured ports. Minimum value = 1
maxconn	<Integer>	Read-write	The maximum number of connections that will be made from the system to the web server(s) attached to it. The value entered here is applied

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			globally to all attached servers. Minimum value = 0 Maximum value = 4294967294
maxreq	<Integer>	Read-write	The maximum number of requests that the system can pass on a particular connection between the system and a server attached to it. Setting this value to 0 allows an unlimited number of requests to be passed. Minimum value = 0 Maximum value = 65535
cip	<String>	Read-write	The option to control (enable or disable) the insertion of the actual client IP address into the HTTP header request passed from the client to one, some, or all servers attached to the system. The passed address can then be accessed through a minor

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			modification to the server. l If cipHeader is specified, it will be used as the client IP header. l If it is not specified, then the value that has been set by the set ns config CLI command will be used as the client IP header. Possible values = ENABLED, DISABLED
cipheader	<String>	Read-write	The text that will be used as the client IP header. Minimum length = 1
cookieversion	<String>	Read-write	The version of the cookie inserted by system. Possible values = 0, 1
securecookie	<String>	Read-write	enable/disable secure flag for persistence cookie. Default value: ENABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ENABLED, DISABLED
pmtumin	<Integer>	Read-write	The minimum Path MTU. Default value: 576 Minimum value = 168 Maximum value = 1500
pmtutimeout	<Integer>	Read-write	The timeout value in minutes. Default value: 10 Minimum value = 1 Maximum value = 1440
ftpportrange	<String>	Read-write	Port range configured for FTP services. Minimum length = 1024 Maximum length = 64000
crportrange	<String>	Read-write	Port range for cache redirection services. Minimum length = 1 Maximum length = 65535

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
timezone	<String>	Read-write	Name of the timezone. Default value: CoordinatedUniversalTime Minimum length = 1 Maximum length = 64
grantquotamaxclient	<Integer>	Read-write	The percentage of shared quota to be granted at a time for maxClient. Default value: 10 Minimum value = 0 Maximum value = 100
exclusivequotamaxclient	<Integer>	Read-write	The percentage of maxClient to be given to PEs. Default value: 80 Minimum value = 0 Maximum value = 100
grantquotaspillover	<Integer>	Read-write	The percentage of shared quota to be granted at a time for spillover. Default value: 10 Minimum value = 0

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum value = 100
exclusivequotaspillover	<Integer>	Read-write	The percentage of spillover threshold to be given to PEs. Default value: 80 Minimum value = 0 Maximum value = 100
securemanagementtraffic	<String>	Read-write	This enabled secure management traffic handling. Default value: DISABLED Possible values = ENABLED, DISABLED
securemanagementtd	<Integer>	Read-write	This positive integer identifies Management traffic domain. If not specified, defaults to 4094. Minimum value = 0 Maximum value = 4094
all	<Boolean>	Read-write	Use this option to do saveconfig for all partitions.
config1	<String>	Read-write	Location of the configurations.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
config2	<String>	Read-write	Location of the configurations.
outtype	<String>	Read-write	Format to display the difference in configurations. Possible values = cli, xml
template	<Boolean>	Read-write	File that contains the commands to be compared.
ignoredevicespecific	<Boolean>	Read-write	Suppress device specific differences.
weakpassword	<Boolean>	Read-write	Option to list all weak passwords (not adhering to strong password requirements). Takes config file as input, if no input specified, running configuration is considered. Command => query ns config -weakpassword / query ns config -weakpassword / nsconfig/ns.conf.
changedpassword	<Boolean>	Read-write	Option to list all passwords changed which would not work when downgraded to older releases. Takes config file as input, if no input specified, running configuration

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			is considered. Command => query ns config -changedpassword / query ns config -changedpassword / nsconfig/ns.conf.
config	<String>	Read-write	configuration File to be used to find weak passwords, if not specified, running config is taken as input.
configfile	<String>	Read-write	Full path of config file to be converted to nitro.
responsefile	<String>	Read-write	Full path of file to store the nitro graph. If not specified, nitro graph is returned as part of the API response.
Async	<Boolean>	Read-write	Using this option will run the operation in async mode and return the job id. The job ID can be used later to track the conversion progress via show ns job <id> Command. This option is mostly useful for API to avoid timeouts for large input configuration.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
message	<String>	Read-only	.
mappedip	<String>	Read-only	Mapped IP Address of the System. Minimum length = 1
range	<Integer>	Read-only	The range of Mapped IP addresses to be configured. Minimum value = 1
svmcmd	<Integer>	Read-only	Identifies the source of command. When SVM fires the nitro command, it will set the value of SVMCMD to be 1 and in other cases it will be 0. Default value: 0
systemtype	<String>	Read-only	The type of the System. Possible Values: Standalone, HA, Cluster. Possible values = Stand-alone, HA, Cluster
primaryip	<String>	Read-only	HA Master Node IP address.
primaryip6	<String>	Read-only	.
flags	<Integer>	Read-only	The flags for this entry.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
lastconfigchangedtime	<String>	Read-only	Time when the configuration was last modified.
lastconfigsavetime	<String>	Read-only	Time when the configuration was last saved through savensconfig.
currentsytemtime	<String>	Read-only	current system time in date format.
systemtime	<Integer>	Read-only	current system time.
configchanged	<Boolean>	Read-only	returns True if configuration has changed since last saved config.
_nextgenapiresource	<String>	Read-only	.
response	<String>	Read-only	.
id	<Integer>	Read-only	Job Id for CLI to Nitro graph request.

Operations

(click to see Properties)

- CLEAR
- UPDATE
- UNSET
- SAVE
- GET (ALL)
- DIFF
- CONVERT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

CLEAR

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsconfig? **action=clear HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nsconfig":{

"force":<Boolean_value>,

<b>"level":<String_value>,

</b>"rbaconfig":<String_value>
```

```
}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsconfig **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nsconfig":{

"ipaddress":<String_value>,

"netmask":<String_value>,

"nsvlan":<Integer_value>,

"ifnum":<String[]_value>,

"tagged":<String_value>,

"httpport":<Integer[]_value>,

"maxconn":<Integer_value>,

"maxreq":<Integer_value>,

"cip":<String_value>,

"cipheader":<String_value>,

"cookieversion":<String_value>,
```

```
"securecookie":<String_value>,

"pmtumin":<Integer_value>,

"pmtutimeout":<Integer_value>,

"ftpportrange":<String_value>,

"crportrange":<String_value>,

"timezone":<String_value>,

"grantquotamaxclient":<Integer_value>,

"exclusivequotamaxclient":<Integer_value>,

"grantquotaspillover":<Integer_value>,

"exclusivequotaspillover":<Integer_value>,

"securemanagementtraffic":<String_value>,

"securemanagementtd":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsconfig? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nsconfig":{

"nsvlan":true,

"securemanagementtraffic":true,

"ftpportrange":true,

"crportrange":true,

"timezone":true,

"ipaddress":true,

"netmask":true,

"ifnum":true,

"tagged":true,

"httpport":true,

"maxconn":true,

"maxreq":true,

"cip":true,

"cipheader":true,

"cookieversion":true,

"securecookie":true,

"pmtumin":true,

"pmtutimeout":true,

"grantquotamaxclient":true,

"exclusivequotamaxclient":true,

"grantquotaspillover":true,
```

```
"exclusivequotaspillover":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

SAVE

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsconfig? **action=save HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nsconfig":{

"all":<Boolean_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DIFF

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsconfig? **action=diff HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nsconfig":{

"config1":<String_value>,

"config2":<String_value>,

"outtype":<String_value>,

"template":<Boolean_value>,

"ignoredevicespecific":<Boolean_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Payload:

```
{ "nsconfig": [ {

"response":<String_value>



}]}
```

CONVERT

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsconfig? **action=convert HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nsconfig":{

<b>"configfile":<String_value>,

</b>"responsefile":<String_value>,

"Async":<Boolean_value>,

"outtype":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsconfig **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nsconfig": [ {

"ipaddress":<String_value>,

"netmask":<String_value>,
```

```
"mappedip":<String_value>,

"range":<Integer_value>,

"nsvlan":<Integer_value>,

"ifnum":<String[]_value>,

"tagged":<String_value>,

"svmcmd":<Integer_value>,

"httpport":<Integer[]_value>,

"maxconn":<Integer_value>,

"maxreq":<Integer_value>,

"cip":<String_value>,

"cipheader":<String_value>,

"cookieversion":<String_value>,

"securecookie":<String_value>,

"failover":<String_value>,

"systemtype":<String_value>,

"primaryip":<String_value>,

"primaryip6":<String_value>,

"pmtumin":<Integer_value>,

"pmtutimeout":<Integer_value>,

"ftpportrange":<String_value>,

"crportrange":<String_value>,

"flags":<Integer_value>,
```

```
"timezone":<String_value>,

"lastconfigchangedtime":<String_value>,

"lastconfigsavetime":<String_value>,

"currentsytemtime":<String_value>,

"systemtime":<Integer_value>,

"grantquotamaxclient":<Integer_value>,

"exclusivequotamaxclient":<Integer_value>,

"grantquotaspillover":<Integer_value>,

"exclusivequotaspillover":<Integer_value>,

"configchanged":<Boolean_value>,

"securemanagementtraffic":<String_value>,

"securemanagementtd":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

nsconfigview

Configuration for 0 resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
state	<String>	Read-write	State is a session-level setting that controls the configuration shown

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			to the user. Based on the selected option user will be able to see only the configuration created through Classic Interface (CLI/API) or Only Configurations created through Next-Gen API, Or both Classic ; Next-Gen API interfaces. Configurations created by Nextgenapi are read-only and can only be modified via Next-Gen API REST endpoints. Configurations created by classic interfaces (CLI, NITRO) are editable for CLASSIC or ALL views. Possible values: - CLASSIC: Config view is limited to the configuration entities created through classic interfaces (CLI, NITRO). This is the default behaviour.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			- NEXTGENAPI: Config view is limited to the configuration entities created through Next-Gen API Interface. - ALL: Configurations created by both Classic and Next-Gen API interfaces are visible. Default value: CLASSIC Possible values = CLASSIC, NEXTGENAPI, ALL
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- SWITCH
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

SWITCH

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsconfigview? **action=Switch HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nsconfigview":{

<b>"state":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsconfigview **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nsconfigview": [ {

"state":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

nsconnectiontable

Configuration for TCP/IP connection table resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
filterexpression	<String>	Read-write	The maximum length of filter expression is 255 and it can be of following format:

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			<expression> [<relop> <expression>] <relop> = (;; | ||) <expression> =: CONNECTION.<qualifier>.<qualifier-method>.(<qualifier-value>) <qualifier> = SRCIP <qualifier-method> = [EQ | NE] <qualifier-value> = A valid IPv4 address example = CONNECTION.SRCIP.EQ(127.0.0.1) <qualifier> = DSTIP <qualifier-method> = [EQ | NE] <qualifier-value> = A valid IPv4 address. example = CONNECTION.DSTIP.EQ(127.0.0.1) <qualifier> = IP

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			<qualifier-method> = [EQ | NE] <qualifier-value> = A valid IPv4 address. example = CONNECTION.IP.EQ(127.0.0.1) <qualifier> = SRCIPv6 <qualifier-method> = [EQ | NE] <qualifier-value> = A valid IPv6 address. example = CONNECTION.SRCIPv6.EQ(2001:db8:0:0:1::1) <qualifier> = DSTIPv6 <qualifier-method> = [EQ | NE] <qualifier-value> = A valid IPv6 address. example = CONNECTION.DST

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			IPv6.EQ(2001:db8:0:0:1::1) <qualifier> = IPv6 <qualifier-method> = [EQ | NE] <qualifier-value> = A valid IPv6 address. example = CONNECTION.IPv6.EQ(2001:db8:0:0:1::1) <qualifier> = SRCPORT <qualifier-method> = [EQ | NE | GT | GE | LT | LE | BETWEEN] <qualifier-value> = A valid port number. example = CONNECTION.SRCPORT.EQ(80) <qualifier> = DSTPORT <qualifier-method> = [EQ | NE | GT | GE | LT | LE

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			| BETWEEN] <qualifier-value> = A valid port number. example = CONNECTION.DSTPORT.EQ(80) <qualifier> = PORT <qualifier-method> = [EQ | NE | GT | GE | LT | LE | BETWEEN] <qualifier-value> = A valid port number. example = CONNECTION.PORT.EQ(80) <qualifier> = SVCNAME <qualifier-method> = [EQ | NE | CONTAINS | STARTSWITH | ENDSWITH] <qualifier-value> = service name. example = CONNECTION.SV

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			CNAME.EQ("name") <qualifier> = LB_VSERVER.NAME <qualifier-method> = [EQ | NE | CONTAINS | STARTSWITH | ENDSWITH] <qualifier-value> = LB vserver name. example = CONNECTION.LB_VSERVER.NAME.EQ("name") <qualifier> = CS_VSERVER.NAME <qualifier-method> = [EQ | NE | CONTAINS | STARTSWITH | ENDSWITH] <qualifier-value> = CS vserver name. example = CONNECTION.CS_

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			VSERVER.NAME.EQ("name") <qualifier> = INTF <qualifier-method> = [EQ | NE] <qualifier-value> = A valid interface id in the form of x/y (n/x/y in case of cluster interface). examle = CONNECTION.INTF.EQ("0/1/1") <qualifier> = VLANID <qualifier-method> = [EQ | NE | GT | GE | LT | LE | BETWEEN] <qualifier-value> = A valid VLAN ID. example = CONNECTION.VLANID.EQ(0) <qualifier> = CONNID

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			<qualifier-method> = [EQ | NE | GT | GE | LT | LE | BETWEEN] <qualifier-value> = A valid PCB dev number. example = CONNECTION.CONNID.EQ(0) <qualifier> = PPEID <qualifier-method> = [EQ | NE | GT | GE | LT | LE | BETWEEN] <qualifier-value> = A valid core ID. example = CONNECTION.PPEID.EQ(0) <qualifier> = IDLETIME <qualifier-method> = [EQ | NE | GT | GE | LT | LE | BETWEEN]

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			<qualifier-value> = A positive integer indicating the idletime. example = CONNECTION.IDLETIME.LT(100) <qualifier> = TCPSTATE <qualifier-method> = [EQ | NE] <qualifier-value> = (CLOSE_WAIT | CLOSED | CLOSING | ESTABLISHED | FIN_WAIT_1 | FIN_WAIT_2 | LAST_ACK | LISTEN | SYN_RECEIVED | SYN_SENT | TIME_WAIT | NOT_APPLICABLE) example = CONNECTION.TCPSTATE.EQ(LISTEN)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			<qualifier> = SERVICE_TYPE <qualifier-method> = [EQ | NE] <qualifier-value> = (SVC_HTTP | FTP | TCP | UDP | SSL | SSL_BRIDGE | SSL_TCP | NNTP | RPCSVR | RPCSVRS | RPCCLNT | SVC_DNS | ADNS | SNMP | RTSP | DHCPRA | NAT | ANY | MONITOR | MONITOR_UDP | MONITOR_PING | SIP_UDP | SVC_MYSQL | SVC_MSSQL | SERVICE_UNKNOWN) example = CONNECTION.SERVICE_TYPE.EQ(ANY)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			<qualifier> = TRAFFIC_DOMAIN_ID <qualifier-method> = [EQ | NE | GT | GE | LT | LE | BETWEEN] <qualifier-value> = A valid traffic domain ID. example = CONNECTION.TRAFFIC_DOMAIN_ID.EQ(0) common usecases: Filtering out loopback connections and view present connections through netscaler show connectiontable "CONNECTION.IP.NE(127.0.0.1) ;; CONNECTION.TCPSTATE.EQ(ESTABLISHED)" -detail full

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			show connections from a particular sourceip and targeted to port 80 show connectiontable "CONNECTION.SRCIP.EQ(10.102.1.91) ;; CONNECTION.DSTPORT.EQ(80)" show connection particular to a service and its linked client connections show connectiontable CONNECTION.SVCNAME.EQ("S1") -detail link show connections for a particular servicetype(e.g.http) show connectiontable CONNECTION.SE

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			RVICE_TYPE.EQ(TCP) viewing connections that have been idle for a long time show connectiontable CONNECTION.IDLETIME.GT(100) show connections particular to a service and idle for a long time show connectiontable "CONNECTION.SVCNAME.EQ(\\"S1\\") ;; CONNECTION.IDLETIME.GT(100)" show connections for a particular interface show connectiontable CONNECTION.INTF.EQ("1/1") show connections for a particular interface and vlan

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			show connectiontable "CONNECTION.INTF.EQ(\\"1/1\\") ;; CONNECTION.VLANID.EQ(1)" .
link	<Boolean>	Read-write	Display link information if available.
filtername	<Boolean>	Read-write	Display name instead of IP for local entities.
detail	<String[]>	Read-write	Specify display options for the connection table. * LINK - Displays the linked PCB (Protocol Control Block). * NAME - Displays along with the service name. * CONNFAILOVER - Displays PCB with connection failover. * FULL - Displays all available details. Possible values = LINK, NAME,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			CONNFAILOVER, FULL, NNM, FULL+
listen	<Boolean>	Read-write	Display listening services only.
nodeid	<Integer>	Read-write	Unique number that identifies the cluster node. Minimum value = 0 Maximum value = 31
sourceip	<String>	Read-only	Source IP of the connection.
sourceport	<Integer>	Read-only	Source port of the connection. Range 1 - 65535 * in CLI is represented as 65535 in NITRO API
destip	<String>	Read-only	Destination IP of the connection.
destport	<Integer>	Read-only	Destination port of the connection. Range 1 - 65535 * in CLI is represented as 65535 in NITRO API
svctype	<String>	Read-only	Protocol supported by the connection.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = HTTP, FTP, TCP, UDP, SSL, SSL_BRIDGE, SSL_TCP, NNTP, RPCSVR, DNS, ADNS, SNMP, RTSP, DHCPRA, ANY, SIP_UDP, SIP_TCP, SIP_SSL, DNS_TCP, ADNS_TCP, HTTPSVR, HTTPCLIENT, NAT, HA, AAA, SINCTCP, VPN AFTP, MONITORS, SSLVPN UDP, SINCUDP, RIP, UDP CLNT, SASP, RPCCLNTS, ROUTE, AUDIT, STA HTTP, STA SSL, DNS RESOLVE, RDP, MYSQL, MSSQL, DIAMETER, SSL_DIAMETER, TFTP, ORACLE, ICA, RADIUS, RADIUSListener, SMPP, PPTP, GRE, SYSLOGTCP, SYSLOGUDP, FIX, SSL_FIX, QUIC, TFTP_DATA,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			USER_TCP, USER_SSL_TCP, MONGO, MONGO_TLS, MQTT, MQTT_TLS, QUIC_BRIDGE, HTTP_QUIC, CT_TCP, CT_UDP, DOT, ADNS_DOT, ADNS_DOH, KAFKA_BROKER, KAFKA_PRODUCER
idletime	<Integer>	Read-only	Time since last activity was detected on the connection.
state	<String>	Read-only	Current TCP/IP state of the connection. Possible values = CLOSED, LISTEN, SYN_SENT, SYN_RECEIVED, ESTABLISHED, CLOSE_WAIT, FIN_WAIT_1, CLOSING, LAST_ACK, FIN_WAIT_2, TIME_WAIT, NA
linksourceip	<String>	Read-only	Source IP of the link connection.
linksourceport	<Integer>	Read-only	Source port of the link connection.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Range 1 - 65535 * in CLI is represented as 65535 in NITRO API
linkdestip	<String>	Read-only	Destination IP of the link connection.
linkdestport	<Integer>	Read-only	Destination port of the link connection. Range 1 - 65535 * in CLI is represented as 65535 in NITRO API
linkservicetype	<String>	Read-only	Protocol supported by the link connection. Possible values = HTTP, FTP, TCP, UDP, SSL, SSL_BRIDGE, SSL_TCP, NNTP, RPCSVR, DNS, ADNS, SNMP, RTSP, DHCPRA, ANY, SIP_UDP, SIP_TCP, SIP_SSL, DNS_TCP, ADNS_TCP, HTTPSVR, HTTPCLIENT, NAT, HA, AAA, SINCTCP, VPN AFTP,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			MONITORS, SSLVPN UDP, SINCUDP, RIP, UDP CLNT, SASP, RPCCLNTS, ROUTE, AUDIT, STA HTTP, STA SSL, DNS RESOLVE, RDP, MYSQL, MSSQL, DIAMETER, SSL_DIAMETER, TFTP, ORACLE, ICA, RADIUS, RADIUSListener, SMPP, PPTP, GRE, SYSLOGTCP, SYSLOGUDP, FIX, SSL_FIX, QUIC, TFTP_DATA, USER_TCP, USER_SSL_TCP, MONGO, MONGO_TLS, MQTT, MQTT_TLS, QUIC_BRIDGE, HTTP_QUIC, CT_TCP, CT_UDP, DOT, ADNS_DOT, ADNS_DOH, KAFKA_BROKER, KAFKA_PRODUCER

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
linkidletime	<Integer>	Read-only	Time since last activity was detected on link connection.
linkstate	<String>	Read-only	TCP/IP current state of link connection. Possible values = CLOSED, LISTEN, SYN_SENT, SYN_RECEIVED, ESTABLISHED, CLOSE_WAIT, FIN_WAIT_1, CLOSING, LAST_ACK, FIN_WAIT_2, TIME_WAIT, NA
entityname	<String>	Read-only	Citrix ADC entity name for the connection.
linkentityname	<String>	Read-only	Citrix ADC entity name for link connection.
connid	<Integer>	Read-only	Unique transaction number for the connection.
linkconnid	<Integer>	Read-only	Unique transaction number for the peer connection.
connproperties	<String[]>	Read-only	flags used to store connection properties like client, server etc.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = LINK, HASLINK, CLIENT, SERVER, NNM, MPTCP, SUBFLOW
optionflags	<String[]>	Read-only	flags used to store TCP options like Sack, WS. Possible values = sack, timstmp, ws
nswsvalue	<Integer>	Read-only	Citrix ADC window scaling value.
peerwsvalue	<Integer>	Read-only	peer window scaling value.
mss	<Integer>	Read-only	Client side MSS for the connection - used in server SYN.
retxretrycnt	<Integer>	Read-only	Retransmission retry count for the connection.
rcvwnd	<Integer>	Read-only	Received Advertised Window for the connection.
advwnd	<Integer>	Read-only	Sent advertised window for the connection.
sndcwnd	<Integer>	Read-only	sent congestion window for the connection.
iss	<Integer>	Read-only	Initial send sequence number for the connection.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
irs	<Integer>	Read-only	Initial receive sequence number for the connection.
rcvnxt	<Integer>	Read-only	next expecting seq number for the connection.
maxack	<Integer>	Read-only	current running max ack sent for the connection.
sndnxt	<Integer>	Read-only	next bytes seq number for the connection.
sndunack	<Integer>	Read-only	Most recently received ACK for the connection.
httpendseq	<Integer>	Read-only	HTTP parsing tracking seq number for the connection.
httpstate	<String>	Read-only	HTTP Protocol state for the connection. Possible values = INITIALIZED, CONTENT_LENGTH, CHUNKED, WAIT_FINAL_ACK, UNKNOWN, DONE, WAIT_FIN
trcount	<Integer>	Read-only	Max reuests allowed per connection.
priority	<String>	Read-only	priority of the connection.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = SC Priority, Priority queue1, priority queue2, priority queue3, DoS Priority, Surge Priority
httpreqver	<String>	Read-only	current HTTP request version on the connection. Possible values = HTTP_1_0, HTTP_1_1, HTTP_0_9, RTSP_1_0, SIP_2_0, VPN_ICA_SOCKS, VPN_ICA_CGP, HTTP_2_0, HTTP_2_0_DIREC T
httprequest	<String>	Read-only	current HTTP request type on the connection. Possible values = OPTIONS, GET, HEAD, POST, PUT, DELETE, TRACE, TRACK, CONNECT, RPCCONNECT
httprspcode	<Integer>	Read-only	current response type on the connection.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
rttsmoothed	<Integer>	Read-only	smoothed RTT value of the connection.
rttvariance	<Integer>	Read-only	RTT variance for the connection.
outoforderpkts	<Integer>	Read-only	held packets on the connection.
linkoptionflag	<String[]>	Read-only	Link connection's TCP option flag for Sack and WS. Possible values = sack, timstmp, ws
linknswsvalue	<Integer>	Read-only	Link connection-s Citrix ADC window scaling value.
linkpeerwsvalue	<Integer>	Read-only	Link connection-s peer Citrix ADC window scaling value.
targetnodeidnnm	<Integer>	Read-only	NNM connection target node ID.
sourcenodeidnnm	<Integer>	Read-only	NNM connection source node ID.
channelidnnm	<Integer>	Read-only	NNM connection channel ID.
msgversionnnm	<Integer>	Read-only	nnm message version.
td	<Integer>	Read-only	Traffic Domain Id.
maxrcvbuf	<Integer>	Read-only	Maximum receive window that

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			application advertizes to peer.
linkmaxrcvbuf	<Integer>	Read-only	Maximum receive window that application advertizes to peer in linked connection.
rxqsize	<Integer>	Read-only	Total number of bytes in Citrix ADC receive buffer. This includes bytes being processed / policy related data / stored in application buffer.
linkrxqsize	<Integer>	Read-only	Total number of bytes in Citrix ADC receive buffer for linked connection. This includes bytes being processed / policy related data / stored in application buffer.
maxsndbuf	<Integer>	Read-only	Maximum send window that application can process and send.
linkmaxsndbuf	<Integer>	Read-only	Maximum send window that application can process and send in linked connection.
txqsize	<Integer>	Read-only	Total number of bytes in Citrix ADC send buffer. This includes both inflight

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			and queued bytes in Citrix ADC.
linktxqsize	<Integer>	Read-only	Total number of bytes in Citrix ADC send buffer for linked connection. This includes both inflight and queued bytes in Citrix ADC.
flavor	<String>	Read-only	TCP congestion control algorithm. Possible values = Default, Westwood, BIC, CUBIC, Nile, BBR
linkflavor	<String>	Read-only	TCP congestion control algorithm for a linked connection. Possible values = Default, Westwood, BIC, CUBIC, Nile, BBR
bwestimate	<Integer>	Read-only	TCP Bandwidth Estimate.
linkbwestimate	<Integer>	Read-only	TCP Bandwidth Estimate for a linked connection.
rttmin	<Integer>	Read-only	Minimum Round Trip Time for the connection.
linkrttmin	<Integer>	Read-only	Minimum Round Trip Time for linked connection.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-only	Name of TCP profile attached to the connection. Minimum length = 1 Maximum length = 127
linkname	<String>	Read-only	Name of TCP profile attached to the connection. Minimum length = 1 Maximum length = 127
tcpmode	<String>	Read-only	TCP Optimization modes TRANSPARENT / ENDPOINT. Possible values = TRANSPARENT, ENDPOINT
linktcpmode	<String>	Read-only	TCP Optimization modes TRANSPARENT / ENDPOINT for linked connection. Possible values = TRANSPARENT, ENDPOINT
realtimertt	<Integer>	Read-only	Real Time / Instantaneous round trip time.
linkrealtimertt	<Integer>	Read-only	Real Time / Instantaneous round

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			trip time for linked connection.
sndbuf	<Integer>	Read-only	send buffer size.
linksndbuf	<Integer>	Read-only	Send buffer size for linked connection.
nsbtcpwaitq	<Integer>	Read-only	Number of packets in TCP wait queue.
linknsbtcpwaitq	<Integer>	Read-only	Number of packets in wait queue for linked connection.
nsbretxq	<Integer>	Read-only	Number of packets in retransmission queue.
linknsbretxq	<Integer>	Read-only	Number of packets in retransmission queue for linked connection.
sackblocks	<Integer>	Read-only	Number of sack blocks attached to the connection.
linksackblocks	<Integer>	Read-only	Number of sack blocks attached in linked connection.
congstate	<String>	Read-only	TCP congestion state. Possible values = open, recovery, loss, reneg, partial_ACK, retx_lost

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
linkcongstate	<String>	Read-only	TCP congestion state for a linked connection. Possible values = open, recovery, loss, reneg, partial_ACK, retx_lost
sndrecoverle	<Integer>	Read-only	Sequence Number denoting end of fast recovery.
linksndrecoverle	<Integer>	Read-only	Sequence Number denoting end of fast recovery for linked connection.
creditsinbytes	<Integer>	Read-only	Connections current credits in Bytes/ms.
linkcredits	<Integer>	Read-only	Link connections current credits in Bytes/ms.
rateinbytes	<Integer>	Read-only	Connections current rate in Bytes/ms.
linkrateinbytes	<Integer>	Read-only	Link connections current rate in Bytes/ms.
rateschedulerqueue	<Integer>	Read-only	Bytes that are queued in the rate scheduler for this connection.
linkrateschedulerqueue	<Integer>	Read-only	Bytes that are queued in the rate

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			scheduler for link connection.
burstratecontrol	<String>	Read-only	TCP Burst Rate Control DISABLED/ FIXED/DYNAMIC. Possible values = DISABLED, FIXED, DYNAMIC
linkburstratecontrol	<String>	Read-only	TCP Burst Rate Control DISABLED/ FIXED/DYNAMIC. Possible values = DISABLED, FIXED, DYNAMIC
cqabifavg	<Integer>	Read-only	Average bytes in flight over maxburst.
cqathruputavg	<Integer>	Read-only	Average instantaneous throughput over maxburst.
cqarcvwndavg	<Integer>	Read-only	Average receive window over maxburst.
cqaiai1mspct	<Integer>	Read-only	Percentage of inter arriaval samples for 1ms over maxburst.
cqaiai2mspct	<Integer>	Read-only	Percentage of inter arriaval samples for 2ms over maxburst.
cqasamples	<Integer>	Read-only	Number of ACK samples over maxburst.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
cqaiaisamples	<Integer>	Read-only	Number of samples considered for calculating inter arrival interval over maxburst.
cqanetclass	<String>	Read-only	Network type name. Maximum length = 49
cqaccl	<Integer>	Read-only	Connection congestion level. Minimum value = 0 Maximum value = 100
cqacsq	<Integer>	Read-only	Connectiontion signal quality level. Minimum value = 0 Maximum value = 100
cqaiaiavg	<Integer>	Read-only	Average inter arriaval interval over maxburst.
cqaisiavg	<Integer>	Read-only	Average inter send interval over maxburst.
cqarcvwndmin	<Integer>	Read-only	Minimum receive window over maxburst.
cqaretxcorr	<Integer>	Read-only	Number of retransmission due to noise over maxburst.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
cqaretxcong	<Integer>	Read-only	Number of retransmission due to congestion over maxburst.
cqaretxpackets	<Integer>	Read-only	Number of retransmission over maxburst.
cqaloaddelayavg	<Integer>	Read-only	Average load delay over maxburst.
cqanoisedelayavg	<Integer>	Read-only	Average noise delay over maxburst.
cqarttmax	<Integer>	Read-only	Maximum RTT sample over maxburst in ms.
cqarttmin	<Integer>	Read-only	Minimum RTT sample over maxburst in ms.
cqarttavg	<Integer>	Read-only	Minimum RTT sample over maxburst in ms.
adaptivetcpprofname	<String>	Read-only	Name of the Adaptive-TCP profile currently assigned to the connection. Minimum length = 1 Maximum length = 127
outoforderblocks	<Integer>	Read-only	held packets on the connection.
outoforderflushedcount	<Integer>	Read-only	held packets on the connection.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
outoforderbytes	<Integer>	Read-only	held packets on the connection.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsconnectiontable **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/nsconnectiontable? **args=filterexpression: <String_value> ,link: <Boolean_value> ,filtername: <Boolean_value> ,detail: <String _value> ,listen: <Boolean_value> ,nodeid: <Integer_value>**

Use this query-parameter to get nsconnectiontable resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/config/nsconnectiontable? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/nsconnectiontable? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of nsconnectiontable resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/nsconnectiontable? **view=summary**

Use this query-parameter to get the summary output of nsconnectiontable resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/nsconnectiontable? **pagesize=#no;pageno=#no**

Use this query-parameter to get the nsconnectiontable resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nsconnectiontable": [ {

filterexpression:<String_value>,link:<Boolean_value>,filtername:<Boolean_v
alue>,detail:<String[]_value>,listen:<Boolean_value>,nodeid:<Integer_value
>"sourceip":<String_value>,

"sourceport":<Integer_value>,

"destip":<String_value>,

"destport":<Integer_value>,

"svctype":<String_value>,

"idletime":<Integer_value>,

"state":<String_value>,

"linksourceip":<String_value>,

"linksourceport":<Integer_value>,

"linkdestip":<String_value>,

"linkdestport":<Integer_value>,

"linkservicetype":<String_value>,

"linkidletime":<Integer_value>,

"linkstate":<String_value>,

"entityname":<String_value>,

"linkentityname":<String_value>,

"connectionnumber":<Integer_value>,

"linkconnectionnumber":<Integer_value>,
```

```
"connid":<Integer_value>,

"linkconnid":<Integer_value>,

"connproperties":<String[]_value>,

"optionflags":<String[]_value>,

"nswsvalue":<Integer_value>,

"peerwsvalue":<Integer_value>,

"mss":<Integer_value>,

"retxretrycnt":<Integer_value>,

"rcvwnd":<Integer_value>,

"advwnd":<Integer_value>,

"sndcwnd":<Integer_value>,

"iss":<Integer_value>,

"irs":<Integer_value>,

"rcvnxt":<Integer_value>,

"maxack":<Integer_value>,

"sndnxt":<Integer_value>,

"sndunack":<Integer_value>,

"httpendseq":<Integer_value>,

"httpstate":<String_value>,

"trcount":<Integer_value>,

"priority":<String_value>,

"httpreqver":<String_value>,
```

```
"httprequest":<String_value>,

"httprspcode":<Integer_value>,

"rttsmoothed":<Integer_value>,

"rttvariance":<Integer_value>,

"outoforderpkts":<Integer_value>,

"linkoptionflag":<String[]_value>,

"linknswsvalue":<Integer_value>,

"linkpeerwsvalue":<Integer_value>,

"targetnodeidnnm":<Integer_value>,

"sourcenodeidnnm":<Integer_value>,

"channelidnnm":<Integer_value>,

"msgversionnnm":<Integer_value>,

"td":<Integer_value>,

"maxrcvbuf":<Integer_value>,

"linkmaxrcvbuf":<Integer_value>,

"rxqsize":<Integer_value>,

"linkrxqsize":<Integer_value>,

"maxsndbuf":<Integer_value>,

"linkmaxsndbuf":<Integer_value>,

"txqsize":<Integer_value>,

"linktxqsize":<Integer_value>,

"flavor":<String_value>,
```

```
"linkflavor":<String_value>,

"bwestimate":<Integer_value>,

"linkbwestimate":<Integer_value>,

"rttmin":<Integer_value>,

"linkrttmin":<Integer_value>,

"name":<String_value>,

"linkname":<String_value>,

"tcpmode":<String_value>,

"linktcpmode":<String_value>,

"realtimertt":<Integer_value>,

"linkrealtimertt":<Integer_value>,

"sndbuf":<Integer_value>,

"linksndbuf":<Integer_value>,

"nsbtcpwaitq":<Integer_value>,

"linknsbtcpwaitq":<Integer_value>,

"nsbretxq":<Integer_value>,

"linknsbretxq":<Integer_value>,

"sackblocks":<Integer_value>,

"linksackblocks":<Integer_value>,

"congstate":<String_value>,

"linkcongstate":<String_value>,

"sndrecoverle":<Integer_value>,
```

```
"linksndrecoverle":<Integer_value>,

"creditsinbytes":<Integer_value>,

"linkcredits":<Integer_value>,

"rateinbytes":<Integer_value>,

"linkrateinbytes":<Integer_value>,

"rateschedulerqueue":<Integer_value>,

"linkrateschedulerqueue":<Integer_value>,

"burstratecontrol":<String_value>,

"linkburstratecontrol":<String_value>,

"cqabifavg":<Integer_value>,

"cqathruputavg":<Integer_value>,

"cqarcvwndavg":<Integer_value>,

"cqaiai1mspct":<Integer_value>,

"cqaiai2mspct":<Integer_value>,

"cqasamples":<Integer_value>,

"cqaiaisamples":<Integer_value>,

"cqanetclass":<String_value>,

"cqaccl":<Integer_value>,

"cqacsq":<Integer_value>,

"cqaiaiavg":<Integer_value>,

"cqaisiavg":<Integer_value>,

"cqarcvwndmin":<Integer_value>,
```

```
"cqaretxcorr":<Integer_value>,

"cqaretxcong":<Integer_value>,

"cqaretxpackets":<Integer_value>,

"cqaloaddelayavg":<Integer_value>,

"cqanoisedelayavg":<Integer_value>,

"cqarttmax":<Integer_value>,

"cqarttmin":<Integer_value>,

"cqarttavg":<Integer_value>,

"adaptivetcpprofname":<String_value>,

"outoforderblocks":<Integer_value>,

"outoforderflushedcount":<Integer_value>,

"outoforderbytes":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsconnectiontable? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nsconnectiontable": [ { "__count": "#no"} ] }
```

nsconsoleloginprompt

Configuration for console prompt resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
promptstring	<String>	Read-write	Console login prompt string.
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- UPDATE
- UNSET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsconsoleloginprompt

HTTP Method: PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nsconsoleloginprompt":{

"promptstring":<String_value>

}}
```

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsconsoleloginprompt? **action=unset**

HTTP Method: POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nsconsoleloginprompt":{

"promptstring":true

}}
```

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsconsoleloginprompt

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nsconsoleloginprompt": [ {

"promptstring":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

nscqaparam

Configuration for cqaparam resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
harqretxdelay	<Integer>	Read-write	HARQ retransmission delay (in ms). Default value: 0 Minimum value = 1 Maximum value = 64000

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
net1label	<String>	Read-write	Name of the network label. Maximum length = 15
minrttnet1	<Integer>	Read-write	MIN RTT (in ms) for the first network. Default value: 0 Minimum value = 0 Maximum value = 6400
lr1coeflist	<String>	Read-write	coefficients values for Label1.
lr1probthresh	<Double>	Read-write	Probability threshold values for LR model to differentiate between NET1 and reset(NET2 and NET3). Default value: 0 Minimum value = 0 Maximum value = 1
net1cclscale	<String>	Read-write	Three congestion level scores limits corresponding to None, Low, Medium.
net1csqscale	<String>	Read-write	Three signal quality level scores limits corresponding to Excellent, Good, Fair.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
net1logcoef	<String>	Read-write	Connection quality ranking Log coefficients of network 1.
net2label	<String>	Read-write	Name of the network label 2. Maximum length = 15
minrttnet2	<Integer>	Read-write	MIN RTT (in ms) for the second network. Default value: 0 Minimum value = 0 Maximum value = 6400
lr2coeflist	<String>	Read-write	coefficients values for Label 2.
lr2probthresh	<Double>	Read-write	Probability threshold values for LR model to differentiate between NET2 and NET3. Default value: 0 Minimum value = 0 Maximum value = 1
net2cclscale	<String>	Read-write	Three congestion level scores limits corresponding to None, Low, Medium.
net2csqscale	<String>	Read-write	Three signal quality level scores limits corresponding to

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Excellent, Good, Fair.
net2logcoef	<String>	Read-write	Connnection quality ranking Log coefficients of network 2.
net3label	<String>	Read-write	Name of the network label 3. Maximum length = 15
minrttnet3	<Integer>	Read-write	MIN RTT (in ms) for the third network. Default value: 0 Minimum value = 0 Maximum value = 6400
net3cclscale	<String>	Read-write	Three congestion level scores limits corresponding to None, Low, Medium.
net3csqscale	<String>	Read-write	Three signal quality level scores limits corresponding to Excellent, Good, Fair.
net3logcoef	<String>	Read-write	Connection quality ranking Log coefficients of network 3.
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- UPDATE
- UNSET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/nscqaparam **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nscqaparam":{

"harqretxdelay":<Integer_value>,

"net1label":<String_value>,

"minrttnet1":<Integer_value>,

"lr1coeflist":<String_value>,

"lr1probthresh":<Double_value>,

"net1cclscale":<String_value>,

"net1csqscale":<String_value>,

"net1logcoef":<String_value>,

"net2label":<String_value>,

"minrttnet2":<Integer_value>,

"lr2coeflist":<String_value>,

"lr2probthresh":<Double_value>,

"net2cclscale":<String_value>,

"net2csqscale":<String_value>,

"net2logcoef":<String_value>,

"net3label":<String_value>,

"minrttnet3":<Integer_value>,

"net3cclscale":<String_value>,

"net3csqscale":<String_value>,

"net3logcoef":<String_value>
```

```
}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/nscqaparam? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nscqaparam":{

"harqretxdelay":true,

"net1label":true,

"minrttnet1":true,

"lr1coeflist":true,

"lr1probthresh":true,

"net1cclscale":true,

"net1csqscale":true,

"net1logcoef":true,

"net2label":true,

"minrttnet2":true,
```

```
"net2cclscale":true,

"net2csqscale":true,

"net2logcoef":true,

"net3label":true,

"minrttnet3":true,

"net3cclscale":true,

"net3csqscale":true,

"net3logcoef":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/nscqaparam **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nscqaparam": [ {

"harqretxdelay":<Integer_value>,

"net1label":<String_value>,

"net2label":<String_value>,

"minrttnet1":<Integer_value>,

"lr1coeflist":<String_value>,

"lr1probthresh":<Double_value>,

"net1cclscale":<String_value>,

"net1csqscale":<String_value>,

"net1logcoef":<String_value>,

"minrttnet2":<Integer_value>,

"lr2coeflist":<String_value>,

"lr2probthresh":<Double_value>,

"net2cclscale":<String_value>,

"net2csqscale":<String_value>,

"net2logcoef":<String_value>,

"net3label":<String_value>,

"minrttnet3":<Integer_value>,

"net3cclscale":<String_value>,

"net3csqscale":<String_value>,

"net3logcoef":<String_value>,

"_nextgenapiresource":<String_value>
```

```
}]}
```

nsdhcpip

Configuration for dhcp IP resource.

Operations

- RELEASE

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

RELEASE

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsdhcpip? **action=release**

HTTP Method: POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nsdhcpip":{

}}
```

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

nsdhcpparams

Configuration for DHCP parameters resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
dhcpclient	<String>	Read-write	Enables DHCP client to acquire IP address from the DHCP server in the next boot. When set to OFF, disables the DHCP client in the next boot. Default value: OFF Possible values = ON, OFF

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
saveroute	<String>	Read-write	DHCP acquired routes are saved on the Citrix ADC. Default value: OFF Possible values = ON, OFF
subnetselection	<String>	Read-write	Subnet Selection option (RFC 3011) to request IP from a specific subnet.
ipaddress	<String>	Read-only	DHCP acquired IP.
netmask	<String>	Read-only	DHCP acquired Netmask.
hostrtgw	<String>	Read-only	DHCP acquired Gateway.
running	<Boolean>	Read-only	DHCP mode.
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- UPDATE
- UNSET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsdhcpparams **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nsdhcpparams":{

"dhcpclient":<String_value>,

"saveroute":<String_value>,

"subnetselection":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsdhcpparams? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nsdhcpparams":{

"dhcpclient":true,

"saveroute":true,

"subnetselection":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsdhcpparams **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nsdhcpparams": [ {

"dhcpclient":<String_value>,

"ipaddress":<String_value>,

"netmask":<String_value>,

"hostrtgw":<String_value>,

"running":<Boolean_value>,

"saveroute":<String_value>,

"subnetselection":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

nsdiameter

Configuration for Diameter Parameters resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
identity	<String>	Read-write	DiameterIdentity to be used by NS. DiameterIdentity is used to identify a Diameter node uniquely. Before setting up diameter

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			configuration, Citrix ADC (as a Diameter node) MUST be assigned a unique DiameterIdentity. example => set ns diameter -identity netscaler.com Now whenever Citrix ADC needs to use identity in diameter messages. It will use 'netscaler.com' as Origin-Host AVP as defined in RFC3588 . Minimum length = 1
realm	<String>	Read-write	Diameter Realm to be used by NS. example => set ns diameter -realm com Now whenever Citrix ADC system needs to use realm in diameter messages. It will use 'com' as Origin-

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Realm AVP as defined in RFC3588 . Minimum length = 1
servercloseproposagation	<String>	Read-write	when a Server connection goes down, whether to close the corresponding client connection if there were requests pending on the server. Default value: NO Possible values = YES, NO
ownernode	<Integer>	Read-write	ID of the cluster node for which the diameter id is set, can be configured only through CLIP. Default value: -1 Minimum value = 0 Maximum value = 31
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- UPDATE

- UNSET
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsdiameter **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nsdiameter":{

"identity":<String_value>,

"realm":<String_value>,

"serverclosepropagation":<String_value>,

"ownernode":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsdiameter? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nsdiameter":{

"serverclosepropagation":true,

"ownernode":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsdiameter **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/nsdiameter? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/nsdiameter? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of nsdiameter resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/nsdiameter? **view=summary**

Use this query-parameter to get the summary output of nsdiameter resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/nsdiameter? **pagesize=#no;pageno=#no**

Use this query-parameter to get the nsdiameter resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nsdiameter": [ {

"ownernode":<Integer_value>,

"identity":<String_value>,

"realm":<String_value>,

"serverclosepropagation":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsdiameter/ ownernode_value<Integer>
Query-parameters: attrs http:// <netscaler-ip-address> /nitro/v1/config/nsdiameter/ ownernode_value<Integer> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/nsdiameter/ ownernode_value<Integer> ? **view=summary**

Use this query-parameter to get the summary output of nsdiameter resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "nsdiameter": [ {

"ownernode":<Integer_value>,

"identity":<String_value>,

"realm":<String_value>,

"serverclosepropagation":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsdiameter? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nsdiameter": [ { "__count": "#no"} ] }
```

nsencryptionkey

Configuration for encryption key resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Key name. This follows the same syntax rules as other expression entity names: It must begin with an alpha character (A-Z or a-z) or an underscore (_). The rest of the characters must be alpha, numeric (0-9) or underscores. It cannot be re or xp (reserved for regular and XPath expressions). It cannot be an expression reserved word (e.g. SYS or HTTP). It cannot be used for an existing expression object (HTTP callout, patset, dataset,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			stringmap, or named expression). Minimum length = 1
method	<String>	Read-write	Cipher method to be used to encrypt and decrypt content. NONE - no encryption or decryption is performed The output of ENCRYPT() and DECRYPT() is the same as the input. RC4 - the RC4 stream cipher with a 128 bit (16 byte) key; RC4 is now considered insecure and should only be used if required by existing applciations. DES[-<mode>] - the Data Encryption Standard (DES) block cipher with a 64-bit (8 byte) key, with 56 data bits and 8 parity bits. DES is considered less secure than DES3 or AES so it should only be used

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			if required by an existing applicastion. The optional mode is described below; DES without a mode is equivalent to DES-CBC. DES3[-<mode>] - the Triple Data Encryption Standard (DES) block cipher with a 192-bit (24 byte) key. The optional mode is described below; DES3 without a mode is equivalent to DES3-CBC. AES<keysize>[-<mode>] - the Advanced Encryption Standard block cipher, available with 128 bit (16 byte), 192 bit (24 byte), and 256 bit (32 byte) keys. The optional mode is described below; AES<keysize> without a mode is equivalent to

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			AES<keysize>-CBC. For a block cipher, the <mode> specifies how multiple blocks of plaintext are encrypted and how the Initialization Vector (IV) is used. Choices are CBC (Cipher Block Chaining) - Each block of plaintext is XORed with the previous ciphertext block, or IV for the first block, before being encrypted. Padding is required if the plaintext is not a multiple of the cipher block size. CFB (Cipher Feedback) - The previous ciphertext block, or the IV for the first block, is encrypted and the output is XORed with the current plaintext block to create the current ciphertext block.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			The 128-bit version of CFB is provided. Padding is not required. OFB (Output Feedback) - A keystream is generated by applying the cipher successfully to the IV and XORing the keystream blocks with the plaintext. Padding is not required. ECB (Electronic Codebook) - Each block of plaintext is independently encrypted. An IV is not used. Padding is required. This mode is considered less secure than the other modes because the same plaintext always produces the same encrypted text and should only be used if required by an existing application. Possible values = NONE, RC4, DES3,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			AES128, AES192, AES256, DES, DES-CBC, DES-CFB, DES-OFB, DES-ECB, DES3-CBC, DES3-CFB, DES3-OFB, DES3-ECB, AES128-CBC, AES128-CFB, AES128-OFB, AES128-ECB, AES192-CBC, AES192-CFB, AES192-OFB, AES192-ECB, AES256-CBC, AES256-CFB, AES256-OFB, AES256-ECB
keyvalue	<String>	Read-write	The hex-encoded key value. The length is determined by the cipher method: RC4 - 16 bytes DES - 8 bytes (all modes) DES3 - 24 bytes (all modes) AES128 - 16 bytes (all modes)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			AES192 - 24 bytes (all modes) AES256 - 32 bytes (all modes) Note that the keyValue will be encrypted when it it is saved. There is a special key value AUTO which generates a new random key for the specified method. This kind of key is intended for use cases where the NetScaler both encrypts and decrypts the same data, such an HTTP header.
padding	<String>	Read-write	Enables or disables the padding of plaintext to meet the block size requirements of block ciphers: ON - For encryption, PKCS5/7 padding is used, which appends n bytes of

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			value n on the end of the plaintext to bring it to the cipher block lnegth. If the plaintext length is alraady a multiple of the block length, an additional block with bytes of value block_length will be added. For decryption, ISO 10126 padding is accepted, which expects the last byte of the block to be the number of added pad bytes. Note that this accepts PKCS5/7 padding, as well as ANSI_X923 padding. Padding ON is the default for the ECB and CBD modes. OFF - No padding. An Undef error will occur with the ECB or CBC modes if the plaintext length is not a multitple of the cipher block size. This can be used with the CFB and

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			OFB modes, and with the ECB and CBC modes if the plaintext will always be an integral number of blocks, or if custom padding is implemented using a policy extension function. Padding OFf is the default for CFB and OFB modes. Default value: DEFAULT Possible values = OFF, ON
iv	<String>	Read-write	The initalization voector (IV) for a block cipher, one block of data used to initialize the encryption. The best practice is to not specify an IV, in which case a new random IV will be generated for each encryption. The format must be iv_data or keyid_iv_data to include the generated IV in the encrypted data. The IV should only be

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			specified if it cannot be included in the encrypted data. The IV length is the cipher block size: RC4 - not used (error if IV is specified) DES - 8 bytes (all modes) DES3 - 8 bytes (all modes) AES128 - 16 bytes (all modes) AES192 - 16 bytes (all modes) AES256 - 16 bytes (all modes).
comment	<String>	Read-write	Comments associated with this encryption key.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- UPDATE
- UNSET
- DELETE

- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.
- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsencryptionkey **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nsencryptionkey":{

<b>"name":<String_value>,

</b><b>"method":<String_value>,

</b>"keyvalue":<String_value>,

"padding":<String_value>,

"iv":<String_value>,

"comment":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsencryptionkey **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nsencryptionkey":{

<b>"name":<String_value>,

</b>"method":<String_value>,

"keyvalue":<String_value>,

"padding":<String_value>,
```

```
"iv":<String_value>,

"comment":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsencryptionkey? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nsencryptionkey":{

<b>"name":<String_value>,

</b>"padding":true,

"iv":true,

"comment":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsencryptionkey/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsencryptionkey **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/nsencryptionkey? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/nsencryptionkey? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of nsencryptionkey resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/nsencryptionkey? **view=summary**

Use this query-parameter to get the summary output of nsencryptionkey resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/nsencryptionkey? **pagesize=#no;pageno=#no**

Use this query-parameter to get the nsencryptionkey resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nsencryptionkey": [ {

"name":<String_value>,

"method":<String_value>,

"padding":<String_value>,

"iv":<String_value>,

"comment":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsencryptionkey/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/nsencryptionkey/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/nsencryptionkey/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of nsencryptionkey resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "nsencryptionkey": [ {

"name":<String_value>,

"method":<String_value>,

"padding":<String_value>,

"iv":<String_value>,

"comment":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsencryptionkey? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nsencryptionkey": [ { "__count": "#no"} ] }
```

nsencryptionparams

Configuration for default encryption parameters resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
method	<String>	Read-write	Cipher method (and key length) to be used to encrypt and decrypt content. The default value is AES256. Possible values = NONE, RC4, DES3, AES128, AES192, AES256, DES, DES-CBC, DES-CFB, DES-OFB, DES-ECB, DES3-CBC, DES3-CFB, DES3-OFB, DES3-ECB, AES128-CBC,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			AES128-CFB, AES128-OFB, AES128-ECB, AES192-CBC, AES192-CFB, AES192-OFB, AES192-ECB, AES256-CBC, AES256-CFB, AES256-OFB, AES256-ECB
keyvalue	<String>	Read-write	The base64-encoded key generation number, method, and key value. Note: * Do not include this argument if you are changing the encryption method. * To generate a new key value for the current encryption method, specify an empty string \(""\) as the value of this parameter. The parameter is passed implicitly, with its automatically generated value, to the Citrix ADC packet engines

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			even when it is not included in the command. Passing the parameter to the packet engines enables the appliance to save the key value to the configuration file and to propagate the key value to the secondary appliance in a high availability setup.
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- UPDATE
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsencryptionparams **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nsencryptionparams":{

<b>"method":<String_value>,

</b>"keyvalue":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsencryptionparams **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nsencryptionparams": [ {

"method":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

nsevents

Configuration for events resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
eventno	<Integer>	Read-write	Event number starting from which events must be shown.
time	<Integer>	Read-only	Event no.
eventcode	<Integer>	Read-only	event Code.
devid	<Integer>	Read-only	Device Name.
devname	<String>	Read-only	Device Name.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
text	<String>	Read-only	Event no.
data0	<Integer>	Read-only	additional event information.
data1	<Integer>	Read-only	additional event information.
data2	<Integer>	Read-only	additional event information.
data3	<Integer>	Read-only	additional event information.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.
- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsevents

Query-parameters:

args

http:// <netscaler-ip-address> /nitro/v1/config/nsevents? **args=eventno: <Integer_value>**

Use this query-parameter to get nsevents resources based on additional properties.

attrs

http:// <netscaler-ip-address> /nitro/v1/config/nsevents? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter

http:// <netscaler-ip-address> /nitro/v1/config/nsevents? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of nsevents resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view

http:// <netscaler-ip-address> /nitro/v1/config/nsevents? **view=summary**

Use this query-parameter to get the summary output of nsevents resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination

http:// <netscaler-ip-address> /nitro/v1/config/nsevents? **pagesize=#no;pageno=#no**

Use this query-parameter to get the nsevents resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nsevents": [ {

eventno:<Integer_value>"time":<Integer_value>,

"eventcode":<Integer_value>,

"devid":<Integer_value>,

"devname":<String_value>,

"text":<String_value>,

"data0":<Integer_value>,

"data1":<Integer_value>,

"data2":<Integer_value>,
```

```
"data3":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsevents? **count=yes**

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nsevents": [ { "__count": "#no"} ] }
```

nsextension

Configuration for Extension resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
src	<String>	Read-write	Local path to and name of, or URL (protocol, host, path, and file name) for, the file in which to store the imported extension. NOTE: The import fails if the object to be imported is on an HTTPS server that requires client certificate authentication for access, and the issuer certificate of the HTTPS server is not present in the specific path on NetScaler to authenticate the HTTPS server. Minimum length = 1 Maximum length = 2047
name	<String>	Read-write	Name to assign to the extension object on the Citrix ADC. Minimum length = 1 Maximum length = 31

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
comment	<String>	Read-write	Any comments to preserve information about the extension object. Maximum length = 128
overwrite	<Boolean>	Read-write	Overwrites the existing file.
trace	<String>	Read-write	Enables tracing to the NS log file of extension execution: off - turns off tracing (equivalent to unset ns extension <extension-name> -trace) calls - traces extension function calls with arguments and function returns with the first return value lines - traces the above plus line numbers for executed extension lines all - traces the above plus local variables changed by executed extension lines

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Note that the DEBUG log level must be enabled to see extension tracing. This can be done by set audit syslogParams -loglevel ALL or -loglevel DEBUG. Default value: off Possible values = off, calls, lines, all
tracefunctions	<String>	Read-write	Comma-separated list of extension functions to trace. By default, all extension functions are traced. Maximum length = 256
tracevariables	<String>	Read-write	Comma-separated list of variables (in traced extension functions) to trace. By default, all variables are traced. Maximum length = 256
detail	<String>	Read-write	Show detail for extension function. Possible values = brief, all

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
type	<String>	Read-only	. Possible values = WSDL, CustomSettings, XMLSchema, XMLErrorPage, htmlpage, CustomResp, Extension, JSONErrorPage, ProtoFile, Signatures, Module
functionhits	<Integer>	Read-only	Number of time function evaluates successfully.
functionundefhits	<Integer>	Read-only	Number of times error occured in evaluating extension function.
functionhaltcount	<Integer>	Read-only	Number of time function evaluation is halted.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- IMPORT
- DELETE
- ADD
- CHANGE

- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

IMPORT

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsextension? **action=Import HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nsextension":{

<b>"src":<String_value>,

</b><b>"name":<String_value>,

</b>"comment":<String_value>,

"overwrite":<Boolean_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsextension/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsextension **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nsextension":{

<b>"name":<String_value>,

</b>"comment":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

CHANGE

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsextension? **action=update HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nsextension":{

<b>"name":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsextension **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nsextension":{

<b>"name":<String_value>,

</b>"trace":<String_value>,

"tracefunctions":<String_value>,

"tracevariables":<String_value>,

"comment":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsextension? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nsextension":{

<b>"name":<String_value>,
```

```
</b>"trace":true,

"tracefunctions":true,

"tracevariables":true,

"comment":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsextension **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/nsextension? **args=name: <String_value> ,detail: <String_value>**

Use this query-parameter to get nsextension resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/config/nsextension? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/nsextension? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of nsextension resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/nsextension? **view=summary**

Use this query-parameter to get the summary output of nsextension resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/nsextension? **pagesize=#no;pageno=#no**

Use this query-parameter to get the nsextension resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nsextension": [ {

name:<String_value>,detail:<String_value>"src":<String_value>,

"type":<String_value>,

"comment":<String_value>,

"functionhits":<Integer_value>,

"functionundefhits":<Integer_value>,

"functionhaltcount":<Integer_value>,

"trace":<String_value>,

"tracefunctions":<String_value>,

"tracevariables":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsextension/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/nsextension/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/nsextension/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of nsextension resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "nsextension": [ {

name:<String_value>,detail:<String_value>"src":<String_value>,

"type":<String_value>,

"comment":<String_value>,
```

```
"functionhits":<Integer_value>,

"functionundefhits":<Integer_value>,

"functionhaltcount":<Integer_value>,

"trace":<String_value>,

"tracefunctions":<String_value>,

"tracevariables":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsextension? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nsextension": [ { "__count": "#no"} ] }
```

nsextension_binding

Binding object which returns the resources bound to nsextension.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the extension object. Minimum length = 1 Maximum length = 31
nsextension_extensionfunction_binding	<nsextension_extensionfunction_binding[]>	Read-only	extensionfunction that can be bound to nsextension.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsextension_binding/ name_value<String>
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nsextension_binding": [ {

"name":<String_value>,

"nsextension_extensionfunction_binding":<nsextension_extensionfunction_binding[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsextension_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/nsextension_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nsextension_binding": [ {

"name":<String_value>,

"nsextension_extensionfunction_binding":<nsextension_extensionfunction_binding[]_value>

}]}
```

nsextension_extensionfunction_binding

Binding object showing the extensionfunction that can be bound to nsextension.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the extension object.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum length = 1 Maximum length = 31
extensionfunctionargcount	<Integer>	Read-only	Number of parameters in the extension function.
extensionfuncdescription	<String>	Read-only	Any description to preserve information about the extension function. Maximum length = 1023
extensionfunctionallparamscount	<Integer>	Read-only	Number of parameters (including promotions) that the function can accept.
extensionfunctionargtype	<String[]>	Read-only	List of extension function's arguments types.
extensionfunctionclasstype	<String>	Read-only	Extension function class type. Minimum length = 1 Maximum length = 31
extensionfunctionreturntype	<String>	Read-only	Extension function return type. Minimum length = 1 Maximum length = 31

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
extensionfunctionallparams	<String[]>	Read-only	List of parameters (including promotions) that the function can accept.
extensionfunctionlinenumber	<Integer>	Read-only	Line number of the function in file.
extensionfunctionclassescount	<Integer>	Read-only	Number of classes the function is present in.
activeextensionfunction	<Integer>	Read-only	Extension function is in use or not.
extensionfunctionclasses	<String[]>	Read-only	List of classes (including inherited) that the function is present in.
extensionfunctionname	<String>	Read-only	Name of extension function given in the extension. Minimum length = 1 Maximum length = 31
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsextension_extensionfunction_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ nsextension_extensionfunction_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of nsextension_extensionfunction_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/nsextension_extensionfunction_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the nsextension_extensionfunction_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "nsextension_extensionfunction_binding": [ {

"name":<String_value>,

"extensionfunctionargcount":<Integer_value>,

"extensionfuncdescription":<String_value>,

"extensionfunctionallparamscount":<Integer_value>,

"extensionfunctionargtype":<String[]_value>,

"extensionfunctionclasstype":<String_value>,

"extensionfunctionreturntype":<String_value>,

"extensionfunctionallparams":<String[]_value>,

"extensionfunctionlinenumber":<Integer_value>,

"extensionfunctionclassescount":<Integer_value>,

"activeextensionfunction":<Integer_value>,

"extensionfunctionclasses":<String[]_value>,

"extensionfunctionname":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsextension_extensionfunction_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/nsextension_extensionfunction_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "nsextension_extensionfunction_binding": [ {

"name":<String_value>,

"extensionfunctionargcount":<Integer_value>,

"extensionfuncdescription":<String_value>,

"extensionfunctionallparamscount":<Integer_value>,

"extensionfunctionargtype":<String[]_value>,

"extensionfunctionclasstype":<String_value>,
```

```
"extensionfunctionreturntype":<String_value>,

"extensionfunctionallparams":<String[]_value>,

"extensionfunctionlinenumber":<Integer_value>,

"extensionfunctionclassescount":<Integer_value>,

"activeextensionfunction":<Integer_value>,

"extensionfunctionclasses":<String[]_value>,

"extensionfunctionname":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsextension_extensionfunction_binding/name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"nsextension_extensionfunction_binding": [ { "__count": "#no"} ] }
```

nsfeature

Configuration for feature resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
feature	<String[]>	Read-write	Feature to be enabled. Multiple features can be specified by providing a blank space between each feature.
wl	<Boolean>	Read-only	Web Logging.
sp	<Boolean>	Read-only	Surge Protection.
lb	<Boolean>	Read-only	Load Balancing.
cs	<Boolean>	Read-only	Content Switching.
cr	<Boolean>	Read-only	Cache Redirect.
cmp	<Boolean>	Read-only	Compression.
ssl	<Boolean>	Read-only	Secure Sockets Layer.
gslb	<Boolean>	Read-only	Global Server Load Balancing.
cf	<Boolean>	Read-only	Content Filter.
ic	<Boolean>	Read-only	Integrated Caching.
sslvpn	<Boolean>	Read-only	SSL VPN.
aaa	<Boolean>	Read-only	AAA.
ospf	<Boolean>	Read-only	OSPF Routing.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
rip	<Boolean>	Read-only	RIP Routing.
bgp	<Boolean>	Read-only	BGP Routing.
rewrite	<Boolean>	Read-only	Rewrite.
ipv6pt	<Boolean>	Read-only	IPv6 protocol translation.
appfw	<Boolean>	Read-only	Application Firewall.
responder	<Boolean>	Read-only	Responder.
push	<Boolean>	Read-only	Citrix ADC Push.
appflow	<Boolean>	Read-only	AppFlow.
cloudbridge	<Boolean>	Read-only	CloudBridge.
isis	<Boolean>	Read-only	ISIS Routing.
ch	<Boolean>	Read-only	Call Home.
appqoe	<Boolean>	Read-only	AppQoS.
contentaccelerator	<Boolean>	Read-only	Transparent Integrated Caching.
feo	<Boolean>	Read-only	Optimize Web content (HTML, CSS, JavaScript, images).
lsn	<Boolean>	Read-only	Large Scale NAT.
rdpproxy	<Boolean>	Read-only	RDPPROXY.
rep	<Boolean>	Read-only	Reputation Services.
videooptimization	<Boolean>	Read-only	Video Optimization.
forwardproxy	<Boolean>	Read-only	Forward Proxy.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
sslinterception	<Boolean>	Read-only	SSL Interception.
adaptivetcp	<Boolean>	Read-only	Adaptive TCP.
cqa	<Boolean>	Read-only	Connection Quality Analytics.
ci	<Boolean>	Read-only	Content Inspection.
bot	<Boolean>	Read-only	Bot Management.
apigateway	<Boolean>	Read-only	API Gateway.
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- ENABLE
- DISABLE
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ENABLE

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsfeature? **action=enable**

HTTP Method: POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nsfeature":{

"feature":<String[]_value>

}}
```

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DISABLE

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsfeature? **action=disable**

HTTP Method: POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nsfeature":{

"feature":<String[]_value>

}}
```

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsfeature

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nsfeature": [ {

"feature":<String[]_value>,

"wl":<Boolean_value>,

"sp":<Boolean_value>,

"lb":<Boolean_value>,

"cs":<Boolean_value>,

"cr":<Boolean_value>,

"cmp":<Boolean_value>,

"ssl":<Boolean_value>,

"gslb":<Boolean_value>,

"routing":<Boolean_value>,

"cf":<Boolean_value>,

"ic":<Boolean_value>,

"sslvpn":<Boolean_value>,

"aaa":<Boolean_value>,

"ospf":<Boolean_value>,

"rip":<Boolean_value>,

"bgp":<Boolean_value>,

"rewrite":<Boolean_value>,

"ipv6pt":<Boolean_value>,

"appfw":<Boolean_value>,

"responder":<Boolean_value>,
```

```
"push":<Boolean_value>,

"appflow":<Boolean_value>,

"cloudbridge":<Boolean_value>,

"isis":<Boolean_value>,

"ch":<Boolean_value>,

"appqoe":<Boolean_value>,

"contentaccelerator":<Boolean_value>,

"feo":<Boolean_value>,

"lsn":<Boolean_value>,

"rdpproxy":<Boolean_value>,

"rep":<Boolean_value>,

"videooptimization":<Boolean_value>,

"forwardproxy":<Boolean_value>,

"sslinterception":<Boolean_value>,

"adaptivetcp":<Boolean_value>,

"cqa":<Boolean_value>,

"ci":<Boolean_value>,

"bot":<Boolean_value>,

"apigateway":<Boolean_value>,

"_nextgenapiresource":<String_value>

}]}
```

nshardware

Configuration for hardware resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
hwdescription	<String>	Read-write	Hardware and it's ports detail.
sysid	<Integer>	Read-write	System id.
manufactureday	<Integer>	Read-write	Manufacturing day.
manufacturemonth	<Integer>	Read-write	Manufacturing month.
manufactureyear	<Integer>	Read-write	Manufacturing year.
cpufrequncy	<Integer>	Read-write	CPU Frequency.
hostid	<Integer>	Read-write	host id.
host	<String>	Read-write	host id.
serialno	<String>	Read-write	Serial no.
encodedserialno	<String>	Read-write	Encoded serial no.
netscaleruuid	<String>	Read-write	Citrix ADC UUID.
bmcrevision	<String>	Read-write	BMC Firmware Revision.
_nextgenapiresource	<String>	Read-write	.

Operations

(click to see Properties)

- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/nshardware

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nshardware": [ {

"hwdescription":<String_value>,

"sysid":<Integer_value>,

"manufactureday":<Integer_value>,

"manufacturemonth":<Integer_value>,

"manufactureyear":<Integer_value>,

"cpufrequncy":<Integer_value>,

"hostid":<Integer_value>,

"host":<String_value>,

"serialno":<String_value>,

"encodedserialno":<String_value>,

"netscaleruuid":<String_value>,

"bmcrevision":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

nshmackey

Configuration for HMAC key resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Key name. This follows the same syntax rules as other expression entity names: It must begin with an alpha character (A-Z or a-z) or an underscore (_). The rest of the characters must be alpha, numeric (0-9) or underscores. It cannot be re or xp (reserved for regular and XPath expressions). It cannot be an expression reserved word (e.g. SYS or HTTP). It cannot be used for an existing expression object (HTTP callout, patset, dataset,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			stringmap, or named expression). Minimum length = 1
digest	<String>	Read-write	Digest (hash) function to be used in the HMAC computation. Possible values = MD2, MD4, MD5, SHA1, SHA224, SHA256, SHA384, SHA512
keyvalue	<String>	Read-write	The hex-encoded key to be used in the HMAC computation. The key can be any length (up to a Citrix ADC-imposed maximum of 255 bytes). If the length is less than the digest block size, it will be zero padded up to the block size. If it is greater than the block size, it will be hashed using the digest function to the block size. The block size for each digest is: MD2 - 16 bytes MD4 - 16 bytes MD5 - 16 bytes

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			SHA1 - 20 bytes SHA224 - 28 bytes SHA256 - 32 bytes SHA384 - 48 bytes SHA512 - 64 bytes Note that the key will be encrypted when it it is saved There is a special key value AUTO which generates a new random key for the specified digest. This kind of key is intended for use cases where the NetScaler both generates and verifies an HMAC on the same data.
comment	<String>	Read-write	Comments associated with this encryption key.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD

- UPDATE
- UNSET
- DELETE
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/nshmackey **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nshmackey":{

<b>"name":<String_value>,

</b><b>"digest":<String_value>,

</b>"keyvalue":<String_value>,

"comment":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/nshmackey **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nshmackey":{

<b>"name":<String_value>,

</b>"digest":<String_value>,

"keyvalue":<String_value>,

"comment":<String_value>
```

```
}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/nshmackey? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nshmackey":{

<b>"name":<String_value>,

</b>"comment":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/nshmackey/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/nshmackey **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/nshmackey? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/nshmackey? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of nshmackey resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/nshmackey? **view=summary**

Use this query-parameter to get the summary output of nshmackey resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/nshmackey? **pagesize=#no;pageno=#no**

Use this query-parameter to get the nshmackey resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nshmackey": [ {

"name":<String_value>,

"digest":<String_value>,

"comment":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/nshmackey/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/nshmackey/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/nshmackey/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of nshmackey resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "nshmackey": [ {

"name":<String_value>,

"digest":<String_value>,

"comment":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/nshmackey? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nshmackey": [ { "__count": "#no"} ] }
```

nshostname

Configuration for host name resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
hostname	<String>	Read-write	Host name for the Citrix ADC. Minimum length = 1 Maximum length = 255
ownernode	<Integer>	Read-write	ID of the cluster node for which you are setting the hostname. Can be configured only through the cluster IP address. Default value: 255 Minimum value = 0 Maximum value = 31
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- UPDATE
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/nshostname **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nshostname":{

<b>"hostname":<String_value>,

</b>"ownernode":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/nshostname **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/nshostname? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/nshostname? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of nshostname resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/nshostname? **view=summary**

Use this query-parameter to get the summary output of nshostname resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/nshostname? **pagesize=#no;pageno=#no**

Use this query-parameter to get the nshostname resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nshostname": [ {

"hostname":<String_value>,

"ownernode":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/nshostname? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nshostname": [ { "__count": "#no"} ] }
```

nshttpparam

Configuration for HTTP parameter resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
dropinvalreqs	<String>	Read-write	Drop invalid HTTP requests or responses. Default value: OFF Possible values = ON, OFF
markhttp09inval	<String>	Read-write	Mark HTTP/0.9 requests as invalid. Default value: OFF Possible values = ON, OFF
markconnreqinval	<String>	Read-write	Mark CONNECT requests as invalid. Default value: OFF Possible values = ON, OFF
insnssrvrhdr	<String>	Read-write	Enable or disable Citrix ADC server header insertion for Citrix ADC generated HTTP responses. Default value: OFF Possible values = ON, OFF
nssrvrhdr	<String>	Read-write	The server header value to be inserted. If no explicit header is specified then NSBUILD.RELEASE

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			is used as default server header. Minimum length = 1
logerrresp	<String>	Read-write	Server header value to be inserted. Default value: ON Possible values = ON, OFF
conmultiplex	<String>	Read-write	Reuse server connections for requests from more than one client connections. Default value: ENABLED Possible values = ENABLED, DISABLED
maxreusepool	<Integer>	Read-write	Maximum limit on the number of connections, from the Citrix ADC to a particular server that are kept in the reuse pool. This setting is helpful for optimal memory utilization and for reducing the idle connections to the server just after the peak time. Default value: 0 Minimum value = 0

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum value = 360000
http2serverside	<String>	Read-write	Enable/Disable HTTP/2 on server side. Default value: OFF Possible values = ON, OFF
ignoreconnectcodingscheme	<String>	Read-write	Ignore Coding scheme in CONNECT request. Default value: DISABLED Possible values = ENABLED, DISABLED
builtin	<String[]>	Read-only	Flag to determine if the http param is built-in or not. Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL
feature	<String>	Read-only	The feature to be checked while applying this config.
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- UPDATE
- UNSET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.
- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/nshttpparam **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nshttpparam":{

"dropinvalreqs":<String_value>,

"markhttp09inval":<String_value>,

"markconnreqinval":<String_value>,

"insnssrvrhdr":<String_value>,

"nssrvrhdr":<String_value>,

"logerrresp":<String_value>,

"conmultiplex":<String_value>,

"maxreusepool":<Integer_value>,

"http2serverside":<String_value>,

"ignoreconnectcodingscheme":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/nshttpparam? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nshttpparam":{

"dropinvalreqs":true,

"markhttp09inval":true,

"markconnreqinval":true,

"insnssrvrhdr":true,

"nssrvrhdr":true,

"logerrresp":true,

"conmultiplex":true,

"maxreusepool":true,

"http2serverside":true,

"ignoreconnectcodingscheme":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/nshttpparam **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nshttpparam": [ {

"dropinvalreqs":<String_value>,

"markhttp09inval":<String_value>,

"markconnreqinval":<String_value>,

"insnssrvrhdr":<String_value>,

"nssrvrhdr":<String_value>,

"logerrresp":<String_value>,

"conmultiplex":<String_value>,

"maxreusepool":<Integer_value>,

"http2serverside":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"ignoreconnectcodingscheme":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

nshttpprofile

Configuration for HTTP profile resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for an HTTP profile. Must begin with a letter, number, or the underscore \(_\) character. Other characters allowed, after the first character, are the hyphen \(-\), period \(.\), hash \(#\), space \(\), at \(@\), colon \(:\), and equal \(=\) characters. The name of a HTTP profile cannot be changed after it is created. CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks \(for example, "my http profile" or 'my http profile'\). Minimum length = 1 Maximum length = 127
dropinvalreqs	<String>	Read-write	Drop invalid HTTP requests or responses. Default value: DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ENABLED, DISABLED
markhttp09inval	<String>	Read-write	Mark HTTP/0.9 requests as invalid. Default value: DISABLED Possible values = ENABLED, DISABLED
markconnreqinval	<String>	Read-write	Mark CONNECT requests as invalid. Default value: DISABLED Possible values = ENABLED, DISABLED
marktracereqinval	<String>	Read-write	Mark TRACE requests as invalid. Default value: DISABLED Possible values = ENABLED, DISABLED
markrfc7230noncompliantinval	<String>	Read-write	Mark RFC7230 non-compliant transaction as invalid. Default value: DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ENABLED, DISABLED
markhttpheaderextrawserror	<String>	Read-write	Mark Http header with extra white space as invalid. Default value: DISABLED Possible values = ENABLED, DISABLED
cmponpush	<String>	Read-write	Start data compression on receiving a TCP packet with PUSH flag set. Default value: DISABLED Possible values = ENABLED, DISABLED
conmultiplex	<String>	Read-write	Reuse server connections for requests from more than one client connections. Default value: ENABLED Possible values = ENABLED, DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
maxreusepool	<Integer>	Read-write	Maximum limit on the number of connections, from the Citrix ADC to a particular server that are kept in the reuse pool. This setting is helpful for optimal memory utilization and for reducing the idle connections to the server just after the peak time. Zero implies no limit on reuse pool size. If non-zero value is given, it has to be greater than or equal to the number of running Packet Engines. Default value: 0 Minimum value = 0 Maximum value = 360000
dropextracrlf	<String>	Read-write	Drop any extra 'CR' and 'LF' characters present after the header. Default value: ENABLED Possible values = ENABLED, DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
incomphdrdelay	<Integer>	Read-write	Maximum time to wait, in milliseconds, between incomplete header packets. If the header packets take longer to arrive at Citrix ADC, the connection is silently dropped. Default value: 7000 Minimum value = 1 Maximum value = 360000
websocket	<String>	Read-write	HTTP connection to be upgraded to a web socket connection. Once upgraded, Citrix ADC does not process Layer 7 traffic on this connection. Default value: DISABLED Possible values = ENABLED, DISABLED
rtsptunnel	<String>	Read-write	Allow RTSP tunnel in HTTP. Once application/x-rtsp-tunnelled is seen in Accept or Content-Type header, Citrix ADC does not process Layer 7

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			traffic on this connection. Default value: DISABLED Possible values = ENABLED, DISABLED
reqtimeout	<Integer>	Read-write	Time, in seconds, within which the HTTP request must complete. If the request does not complete within this time, the specified request timeout action is executed. Zero disables the timeout. Default value: 0 Minimum value = 0 Maximum value = 86400
adpttimeout	<String>	Read-write	Adapts the configured request timeout based on flow conditions. The timeout is increased or decreased internally and applied on the flow. Default value: DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ENABLED, DISABLED
reqtimeoutaction	<String>	Read-write	Action to take when the HTTP request does not complete within the specified request timeout duration. You can configure the following actions: * RESET - Send RST (reset) to client when timeout occurs. * DROP - Drop silently when timeout occurs. * Custom responder action - Name of the responder action to trigger when timeout occurs, used to send custom message.
dropextradata	<String>	Read-write	Drop any extra data when server sends more data than the specified content-length. Default value: DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ENABLED, DISABLED
weblog	<String>	Read-write	Enable or disable web logging. Default value: ENABLED Possible values = ENABLED, DISABLED
clientiphdrexpr	<String>	Read-write	Name of the header that contains the real client IP address.
maxreq	<Integer>	Read-write	Maximum number of requests allowed on a single connection. Zero implies no limit on the number of requests. Default value: 0 Minimum value = 0 Maximum value = 65534
persistentetag	<String>	Read-write	Generate the persistent Citrix ADC specific ETag for the HTTP response with ETag header. Default value: DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ENABLED, DISABLED
http2	<String>	Read-write	Choose whether to enable support for HTTP/2. Default value: DISABLED Possible values = ENABLED, DISABLED
http2direct	<String>	Read-write	Choose whether to enable support for Direct HTTP/2. Default value: DISABLED Possible values = ENABLED, DISABLED
http2strictcipher	<String>	Read-write	Choose whether to enable strict HTTP/2 cipher selection. Default value: ENABLED Possible values = ENABLED, DISABLED
http2altsvcframe	<String>	Read-write	Choose whether to enable support for sending HTTP/2 ALTSVC frames. When enabled, the ADC sends HTTP/2

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			ALTSVC frames to HTTP/2 clients, instead of the Alt-Svc response header field. Not applicable to servers. Default value: DISABLED Possible values = ENABLED, DISABLED
altsvc	<String>	Read-write	Choose whether to enable support for Alternative Services. Default value: DISABLED Possible values = ENABLED, DISABLED
altsvcvalue	<String>	Read-write	Configure a custom Alternative Services header value that should be inserted in the response to advertise a HTTP/SSL/HTTP_QUIC vserver.
reusepooltimeout	<Integer>	Read-write	Idle timeout (in seconds) for server connections in re-use pool. Connections in the re-use pool are flushed, if they

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			remain idle for the configured timeout. Default value: 0 Minimum value = 0 Maximum value = 31536000
maxheaderlen	<Integer>	Read-write	Number of bytes to be queued to look for complete header before returning error. If complete header is not obtained after queuing these many bytes, request will be marked as invalid and no L7 processing will be done for that TCP connection. Default value: 24820 Minimum value = 2048 Maximum value = 122880
maxheaderfieldlen	<Integer>	Read-write	Number of bytes allowed for header field for HTTP header. If number of bytes exceeds beyond configured value, then request will be marked invalid.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: 24820 Minimum value = 2048 Maximum value = 122880
minreusepool	<Integer>	Read-write	Minimum limit on the number of connections, from the Citrix ADC to a particular server that are kept in the reuse pool. This setting is helpful for optimal memory utilization and for reducing the idle connections to the server just after the peak time. Zero implies no limit on reuse pool size. Default value: 0 Minimum value = 0 Maximum value = 360000
http2maxheaderlistsize	<Integer>	Read-write	Maximum size of header list that the Citrix ADC is prepared to accept, in bytes. NOTE: The actual plain text header size that the Citrix ADC accepts is limited by maxHeaderLen.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Please change maxHeaderLen parameter as well when modifying http2MaxHeaderList Size. Default value: 24576 Minimum value = 8192 Maximum value = 131071
http2maxframesize	<Integer>	Read-write	Maximum size of the frame payload that the Citrix ADC is willing to receive, in bytes. Default value: 16384 Minimum value = 16384 Maximum value = 32768
http2maxconcurrents treams	<Integer>	Read-write	Maximum number of concurrent streams that is allowed per connection. Default value: 100 Minimum value = 0 Maximum value = 1000

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
http2initialconnwindowsize	<Integer>	Read-write	Initial window size for connection level flow control, in bytes. Default value: 65535 Minimum value = 65535 Maximum value = 67108864
http2initialwindowsize	<Integer>	Read-write	Initial window size for stream level flow control, in bytes. Default value: 65535 Minimum value = 8192 Maximum value = 20971520
http2headertablesize	<Integer>	Read-write	Maximum size of the header compression table used to decode header blocks, in bytes. Default value: 4096 Minimum value = 0 Maximum value = 131072
http2minseverconn	<Integer>	Read-write	Minimum number of HTTP2 connections established to backend server, on receiving HTTP

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			requests from client before multiplexing the streams into the available HTTP/2 connections. Default value: 20 Minimum value = 1 Maximum value = 360000
http2maxpingframespermin	<Integer>	Read-write	Maximum number of PING frames allowed in HTTP2 connection per minute. Default value: 60 Minimum value = 1 Maximum value = 360000
http2maxsettingsframespermin	<Integer>	Read-write	Maximum number of SETTINGS frames allowed in HTTP2 connection per minute. Default value: 15 Minimum value = 1 Maximum value = 360000
http2maxresetframespermin	<Integer>	Read-write	Maximum number of outgoing RST_STREAM frames allowed in HTTP/2 connection per minute.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: 90 Minimum value = 1 Maximum value = 360000
http2maxemptyframespermin	<Integer>	Read-write	Maximum number of empty frames allowed in HTTP2 connection per minute. Default value: 60 Minimum value = 1 Maximum value = 360000
http2maxrxresetframespermin	<Integer>	Read-write	Maximum number of incoming RST_STREAM frames allowed in HTTP/2 connection per minute. Default value: 0 Minimum value = 0 Maximum value = 360000
http2smallwndtimeout	<Integer>	Read-write	Timeout in seconds for HTTP/2 small window stalled streams. Connection is silently closed if a stream remains stalled with zero or small window for this

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			duration. 0 disables the check. Default value: 0 Minimum value = 0 Maximum value = 18000
grpcholdlimit	<Integer>	Read-write	Maximum size in bytes allowed to buffer gRPC packets till trailer is received. Default value: 131072 Minimum value = 0 Maximum value = 33554432
grpcholdtimeout	<Integer>	Read-write	Maximum time in milliseconds allowed to buffer gRPC packets till trailer is received. The value should be in multiples of 100. Default value: 1000 Minimum value = 0 Maximum value = 180000
grpclengthdelimitation	<String>	Read-write	Set to DISABLED for gRPC without a length delimitation. Default value: ENABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ENABLED, DISABLED
apdexcltresptimethreshold	<Integer>	Read-write	This option sets the satisfactory threshold (T) for client response time in milliseconds to be used for APDEX calculations. This means a transaction responding in less than this threshold is considered satisfactory. Transaction responding between T and 4*T is considered tolerable. Any transaction responding in more than 4*T time is considered frustrating. Citrix ADC maintains stats for such tolerable and frustrating transcations. And client response time related apdex counters are only updated on a vserver which receives clients traffic. Default value: 500 Minimum value = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum value = 3600000
http3	<String>	Read-write	Choose whether to enable support for HTTP/3. Default value: DISABLED Possible values = ENABLED, DISABLED
http3maxheaderfieldsectionsize	<Integer>	Read-write	Maximum size of the HTTP/3 header field section, in bytes. Default value: 24576 Minimum value = 8192 Maximum value = 131072
http3maxheadertablesize	<Integer>	Read-write	Maximum size of the HTTP/3 QPACK dynamic header table, in bytes. Default value: 4096 Minimum value = 0 Maximum value = 131072
http3maxheaderblockedstreams	<Integer>	Read-write	Maximum number of HTTP/3 streams that can be blocked while

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			HTTP/3 headers are being decoded. Default value: 100 Minimum value = 1 Maximum value = 500
http3webtransport	<String>	Read-write	Choose whether to enable support for WebTransport over HTTP/3. Default value: DISABLED Possible values = ENABLED, DISABLED
http3minseverconn	<Integer>	Read-write	Minimum number of HTTP/3 connections established to backend server, on receiving HTTP requests from client before multiplexing the streams into the available HTTP/3 connections. Default value: 20 Minimum value = 1 Maximum value = 360000
httppipelinebuffsize	<Integer>	Read-write	Application pipeline request buffering size, in bytes.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: 131072 Minimum value = 131072 Maximum value = 20971520
allowonlywordcharactersandhyphen	<String>	Read-write	When enabled allows only the word characters [A-Za-z0-9_] and hyphen [-] in the request/response header names and the connection will be reset for the other characters. When disabled allows any visible (printing) characters (%21-%7E) except delimiters (double quotes and "(),/:;<=>?@[]{}"). Default value: DISABLED Possible values = ENABLED, DISABLED
hostheadervalidation	<String>	Read-write	Validates the length of the Host header and its syntax. Also includes validation of the port number if specified.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: DISABLED Possible values = ENABLED, DISABLED
maxduplicateheaderfields	<Integer>	Read-write	Maximum number of allowed occurrences of header fields that share the same field name. This threshold is enforced only for well-known header field names recognized by NetScaler. If the value is set to 0, then it will be similar to previous behavior, Where we store only 15 duplicate headers and rest are parsed and send to the server. Default value: 0 Minimum value = 0 Maximum value = 15
passprotocolupgrade	<String>	Read-write	Pass protocol upgrade request to the server. Default value: ENABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ENABLED, DISABLED
http2extendedconnect	<String>	Read-write	Choose whether to enable HTTP/2 Extended CONNECT mechanism. Default value: ENABLED Possible values = ENABLED, DISABLED
normalizeurl	<String>	Read-write	Enable or disable RFC 3986 normalization of incoming URL before validation or consumption. Default value: DISABLED Possible values = ENABLED, DISABLED
normalizeurltoorigin	<String>	Read-write	Enable or disable RFC 3986 URL normalization for request sent to the origin server. Default value: DISABLED Possible values = ENABLED, DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
refcnt	<Integer>	Read-only	Number of entities using this profile.
builtin	<String[]>	Read-only	Flag to determine if http profile is built-in or not. Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL
apdexsvrresptimethreshold	<Integer>	Read-only	This option sets the satisfactory threshold (T) for server response time in milliseconds to be used for APDEX calculations. This means a transaction responding in less than this threshold is considered satisfactory. Transaction responding between T and 4*T is considered tolerable. Any transaction responding in more than 4*T time is considered frustrating. Citrix ADC maintains stats for such tolerable and frustrating transcations. Server Response time related apdex counters are only

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			updated on backend services or a backend vserver which is not accepting client traffic. Default value: 400 Minimum value = 1 Maximum value = 3600000
dropinvalreqswarning	<String>	Read-only	Display warning if Drop invalid reqs is disabled in the profile. Default value: 0 Possible values = Secure deployment guide : This http profile is insecure. To keep it secure enable - Drop invalid HTTP requests
feature	<String>	Read-only	The feature to be checked while applying this config.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD

- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/nshttpprofile **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nshttpprofile":{

<b>"name":<String_value>,

</b>"dropinvalreqs":<String_value>,

"markhttp09inval":<String_value>,

"markconnreqinval":<String_value>,

"marktracereqinval":<String_value>,

"markrfc7230noncompliantinval":<String_value>,

"markhttpheaderextrawserror":<String_value>,

"cmponpush":<String_value>,

"conmultiplex":<String_value>,

"maxreusepool":<Integer_value>,

"dropextracrlf":<String_value>,

"incomphdrdelay":<Integer_value>,

"websocket":<String_value>,

"rtsptunnel":<String_value>,

"reqtimeout":<Integer_value>,

"adpttimeout":<String_value>,

"reqtimeoutaction":<String_value>,

"dropextradata":<String_value>,

"weblog":<String_value>,
```

```
"clientiphdrexpr":<String_value>,

"maxreq":<Integer_value>,

"persistentetag":<String_value>,

"http2":<String_value>,

"http2direct":<String_value>,

"http2strictcipher":<String_value>,

"http2altsvcframe":<String_value>,

"altsvc":<String_value>,

"altsvcvalue":<String_value>,

"reusepooltimeout":<Integer_value>,

"maxheaderlen":<Integer_value>,

"maxheaderfieldlen":<Integer_value>,

"minreusepool":<Integer_value>,

"http2maxheaderlistsize":<Integer_value>,

"http2maxframesize":<Integer_value>,

"http2maxconcurrentstreams":<Integer_value>,

"http2initialconnwindowsize":<Integer_value>,

"http2initialwindowsize":<Integer_value>,

"http2headertablesize":<Integer_value>,

"http2minseverconn":<Integer_value>,

"http2maxpingframespermin":<Integer_value>,

"http2maxsettingsframespermin":<Integer_value>,
```

```
"http2maxresetframespermin":<Integer_value>,

"http2maxemptyframespermin":<Integer_value>,

"http2maxrxresetframespermin":<Integer_value>,

"http2smallwndtimeout":<Integer_value>,

"grpcholdlimit":<Integer_value>,

"grpcholdtimeout":<Integer_value>,

"grpclengthdelimitation":<String_value>,

"apdexcltresptimethreshold":<Integer_value>,

"http3":<String_value>,

"http3maxheaderfieldsectionsize":<Integer_value>,

"http3maxheadertablesize":<Integer_value>,

"http3maxheaderblockedstreams":<Integer_value>,

"http3webtransport":<String_value>,

"http3minseverconn":<Integer_value>,

"httppipelinebuffsize":<Integer_value>,

"allowonlywordcharactersandhyphen":<String_value>,

"hostheadervalidation":<String_value>,

"maxduplicateheaderfields":<Integer_value>,

"passprotocolupgrade":<String_value>,

"http2extendedconnect":<String_value>,

"normalizeurl":<String_value>,

"normalizeurltoorigin":<String_value>
```

```
}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/nshttpprofile/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/nshttpprofile **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nshttpprofile":{

<b>"name":<String_value>,

</b>"dropinvalreqs":<String_value>,

"markhttp09inval":<String_value>,

"markconnreqinval":<String_value>,

"marktracereqinval":<String_value>,
```

```
"markrfc7230noncompliantinval":<String_value>,

"markhttpheaderextrawserror":<String_value>,

"cmponpush":<String_value>,

"conmultiplex":<String_value>,

"maxreusepool":<Integer_value>,

"dropextracrlf":<String_value>,

"incomphdrdelay":<Integer_value>,

"websocket":<String_value>,

"rtsptunnel":<String_value>,

"reqtimeout":<Integer_value>,

"adpttimeout":<String_value>,

"reqtimeoutaction":<String_value>,

"dropextradata":<String_value>,

"weblog":<String_value>,

"clientiphdrexpr":<String_value>,

"maxreq":<Integer_value>,

"persistentetag":<String_value>,

"http2":<String_value>,

"http2direct":<String_value>,

"http2strictcipher":<String_value>,

"http2altsvcframe":<String_value>,

"altsvc":<String_value>,
```

```
"altsvcvalue":<String_value>,

"http2maxheaderlistsize":<Integer_value>,

"http2maxframesize":<Integer_value>,

"http2maxconcurrentstreams":<Integer_value>,

"http2initialconnwindowsize":<Integer_value>,

"http2initialwindowsize":<Integer_value>,

"http2headertablesize":<Integer_value>,

"http2minseverconn":<Integer_value>,

"http2maxpingframespermin":<Integer_value>,

"http2maxsettingsframespermin":<Integer_value>,

"http2maxresetframespermin":<Integer_value>,

"http2maxemptyframespermin":<Integer_value>,

"http2maxrxresetframespermin":<Integer_value>,

"http2smallwndtimeout":<Integer_value>,

"grpcholdlimit":<Integer_value>,

"grpcholdtimeout":<Integer_value>,

"grpclengthdelimitation":<String_value>,

"reusepooltimeout":<Integer_value>,

"maxheaderlen":<Integer_value>,

"maxheaderfieldlen":<Integer_value>,

"minreusepool":<Integer_value>,

"apdexcltresptimethreshold":<Integer_value>,
```

```
"http3":<String_value>,

"http3maxheaderfieldsectionsize":<Integer_value>,

"http3maxheadertablesize":<Integer_value>,

"http3maxheaderblockedstreams":<Integer_value>,

"http3webtransport":<String_value>,

"http3minseverconn":<Integer_value>,

"httppipelinebuffsize":<Integer_value>,

"allowonlywordcharactersandhyphen":<String_value>,

"hostheadervalidation":<String_value>,

"maxduplicateheaderfields":<Integer_value>,

"passprotocolupgrade":<String_value>,

"http2extendedconnect":<String_value>,

"normalizeurl":<String_value>,

"normalizeurltoorigin":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/nshttpprofile? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nshttpprofile":{

<b>"name":<String_value>,

</b>"dropinvalreqs":true,

"markhttp09inval":true,

"markconnreqinval":true,

"marktracereqinval":true,

"markrfc7230noncompliantinval":true,

"markhttpheaderextrawserror":true,

"cmponpush":true,

"conmultiplex":true,

"maxreusepool":true,

"dropextracrlf":true,

"incomphdrdelay":true,

"websocket":true,

"dropextradata":true,

"clientiphdrexpr":true,

"reqtimeout":true,

"adpttimeout":true,

"reqtimeoutaction":true,
```

```
"weblog":true,

"maxreq":true,

"persistentetag":true,

"http2":true,

"http2maxheaderlistsize":true,

"http2maxframesize":true,

"http2maxconcurrentstreams":true,

"http2initialwindowsize":true,

"http2headertablesize":true,

"http2minseverconn":true,

"http2maxpingframespermin":true,

"http2maxsettingsframespermin":true,

"http2maxresetframespermin":true,

"http2maxemptyframespermin":true,

"http2maxrxresetframespermin":true,

"http2smallwndtimeout":true,

"http2altsvcframe":true,

"altsvcvalue":true,

"reusepooltimeout":true,

"maxheaderlen":true,

"rtsptunnel":true,

"minreusepool":true,
```

```
"apdexcltresptimethreshold":true,

"http3":true,

"http3maxheaderfieldsectionsize":true,

"http3maxheadertablesize":true,

"http3maxheaderblockedstreams":true,

"http3webtransport":true,

"http3minseverconn":true,

"httppipelinebuffsize":true,

"allowonlywordcharactersandhyphen":true,

"hostheadervalidation":true,

"maxduplicateheaderfields":true,

"passprotocolupgrade":true,

"normalizeurl":true,

"normalizeurltoorigin":true,

"http2direct":true,

"http2strictcipher":true,

"altsvc":true,

"http2initialconnwindowsize":true,

"grpcholdlimit":true,

"grpcholdtimeout":true,

"grpclengthdelimitation":true,

"maxheaderfieldlen":true,
```

```
"http2extendedconnect":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/nshttpprofile **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/nshttpprofile? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/nshttpprofile? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of nshttpprofile resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/nshttpprofile? **view=summary**

Use this query-parameter to get the summary output of nshttpprofile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/nshttpprofile? **pagesize=#no;pageno=#no**

Use this query-parameter to get the nshttpprofile resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nshttpprofile": [ {

"name":<String_value>,

"dropinvalreqs":<String_value>,

"markhttp09inval":<String_value>,

"markconnreqinval":<String_value>,

"marktracereqinval":<String_value>,

"markrfc7230noncompliantinval":<String_value>,

"markhttpheaderextrawserror":<String_value>,

"cmponpush":<String_value>,

"conmultiplex":<String_value>,

"maxreusepool":<Integer_value>,

"websocket":<String_value>,

"refcnt":<Integer_value>,

"dropextracrlf":<String_value>,

"incomphdrdelay":<Integer_value>,

"reqtimeout":<Integer_value>,

"adpttimeout":<String_value>,
```

```
"reqtimeoutaction":<String_value>,

"dropextradata":<String_value>,

"weblog":<String_value>,

"clientiphdrexpr":<String_value>,

"maxreq":<Integer_value>,

"persistentetag":<String_value>,

"http2":<String_value>,

"http2direct":<String_value>,

"http2strictcipher":<String_value>,

"http2altsvcframe":<String_value>,

"altsvc":<String_value>,

"altsvcvalue":<String_value>,

"http2maxheaderlistsize":<Integer_value>,

"http2maxframesize":<Integer_value>,

"http2maxconcurrentstreams":<Integer_value>,

"http2initialconnwindowsize":<Integer_value>,

"http2initialwindowsize":<Integer_value>,

"http2headertablesize":<Integer_value>,

"http2minseverconn":<Integer_value>,

"http2maxpingframespermin":<Integer_value>,

"http2maxsettingsframespermin":<Integer_value>,

"http2maxresetframespermin":<Integer_value>,
```

```
"http2maxemptyframespermin":<Integer_value>,

"http2maxrxresetframespermin":<Integer_value>,

"http2smallwndtimeout":<Integer_value>,

"grpcholdlimit":<Integer_value>,

"grpcholdtimeout":<Integer_value>,

"grpclengthdelimitation":<String_value>,

"reusepooltimeout":<Integer_value>,

"maxheaderlen":<Integer_value>,

"maxheaderfieldlen":<Integer_value>,

"rtsptunnel":<String_value>,

"minreusepool":<Integer_value>,

"builtin":<String[]_value>,

"apdexsvrresptimethreshold":<Integer_value>,

"apdexcltresptimethreshold":<Integer_value>,

"http3":<String_value>,

"http3maxheaderfieldsectionsize":<Integer_value>,

"http3maxheadertablesize":<Integer_value>,

"http3maxheaderblockedstreams":<Integer_value>,

"http3webtransport":<String_value>,

"httppipelinebuffsize":<Integer_value>,

"normalizeurl":<String_value>,

"normalizeurltoorigin":<String_value>,
```

```
"allowonlywordcharactersandhyphen":<String_value>,

"hostheadervalidation":<String_value>,

"maxduplicateheaderfields":<Integer_value>,

"http3minseverconn":<Integer_value>,

"dropinvalreqswarning":<String_value>,

"passprotocolupgrade":<String_value>,

"feature":<String_value>,

"http2extendedconnect":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/nshttpprofile/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/nshttpprofile/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/nshttpprofile/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of nshttpprofile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "nshttpprofile": [ {

"name":<String_value>,

"dropinvalreqs":<String_value>,

"markhttp09inval":<String_value>,

"markconnreqinval":<String_value>,

"marktracereqinval":<String_value>,

"markrfc7230noncompliantinval":<String_value>,

"markhttpheaderextrawserror":<String_value>,

"cmponpush":<String_value>,

"conmultiplex":<String_value>,

"maxreusepool":<Integer_value>,

"websocket":<String_value>,

"refcnt":<Integer_value>,

"dropextracrlf":<String_value>,

"incomphdrdelay":<Integer_value>,

"reqtimeout":<Integer_value>,

"adpttimeout":<String_value>,
```

```
"reqtimeoutaction":<String_value>,

"dropextradata":<String_value>,

"weblog":<String_value>,

"clientiphdrexpr":<String_value>,

"maxreq":<Integer_value>,

"persistentetag":<String_value>,

"http2":<String_value>,

"http2direct":<String_value>,

"http2strictcipher":<String_value>,

"http2altsvcframe":<String_value>,

"altsvc":<String_value>,

"altsvcvalue":<String_value>,

"http2maxheaderlistsize":<Integer_value>,

"http2maxframesize":<Integer_value>,

"http2maxconcurrentstreams":<Integer_value>,

"http2initialconnwindowsize":<Integer_value>,

"http2initialwindowsize":<Integer_value>,

"http2headertablesize":<Integer_value>,

"http2minseverconn":<Integer_value>,

"http2maxpingframespermin":<Integer_value>,

"http2maxsettingsframespermin":<Integer_value>,

"http2maxresetframespermin":<Integer_value>,
```

```
"http2maxemptyframespermin":<Integer_value>,

"http2maxrxresetframespermin":<Integer_value>,

"http2smallwndtimeout":<Integer_value>,

"grpcholdlimit":<Integer_value>,

"grpcholdtimeout":<Integer_value>,

"grpclengthdelimitation":<String_value>,

"reusepooltimeout":<Integer_value>,

"maxheaderlen":<Integer_value>,

"maxheaderfieldlen":<Integer_value>,

"rtsptunnel":<String_value>,

"minreusepool":<Integer_value>,

"builtin":<String[]_value>,

"apdexsvrresptimethreshold":<Integer_value>,

"apdexcltresptimethreshold":<Integer_value>,

"http3":<String_value>,

"http3maxheaderfieldsectionsize":<Integer_value>,

"http3maxheadertablesize":<Integer_value>,

"http3maxheaderblockedstreams":<Integer_value>,

"http3webtransport":<String_value>,

"httppipelinebuffsize":<Integer_value>,

"normalizeurl":<String_value>,

"normalizeurltoorigin":<String_value>,
```

```
"allowonlywordcharactersandhyphen":<String_value>,

"hostheadervalidation":<String_value>,

"maxduplicateheaderfields":<Integer_value>,

"http3minseverconn":<Integer_value>,

"dropinvalreqswarning":<String_value>,

"passprotocolupgrade":<String_value>,

"feature":<String_value>,

"http2extendedconnect":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/nshttpprofile? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nshttpprofile": [ { "__count": "#no"} ] }
```

nsicapprofile

Configuration for ICAP profile resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for an ICAP profile. Must begin with a letter, number, or the underscore \(_\) character. Other characters allowed, after the first character, are the hyphen \(-\), period \(.\), hash \(#\), space \(\), at \(@\), colon \(:\), and equal \(=\) characters. The name of a ICAP profile cannot be changed after it is created. CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks \(for example, "my icap profile" or 'my icap profile'\). Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum length = 127
preview	<String>	Read-write	Enable or Disable preview header with ICAP request. This feature allows an ICAP server to see the beginning of a transaction, then decide if it wants to opt-out of the transaction early instead of receiving the remainder of the request message. Default value: DISABLED Possible values = ENABLED, DISABLED
previewlength	<Integer>	Read-write	Value of Preview Header field. Citrix ADC uses the minimum of this set value and the preview size received on OPTIONS response. Default value: 4096 Minimum value = 0 Maximum value = 4294967294
uri	<String>	Read-write	URI representing icap service. It is a mandatory argument

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			while creating an icapprofile. Minimum length = 1
hostheader	<String>	Read-write	ICAP Host Header. Minimum length = 1
useragent	<String>	Read-write	ICAP User Agent Header String. Minimum length = 1
mode	<String>	Read-write	ICAP Mode of operation. It is a mandatory argument while creating an icapprofile. Possible values = REQMOD, RESPMOD
queryparams	<String>	Read-write	Query parameters to be included with ICAP request URI. Entered values should be in arg=value format. For more than one parameters, add ; separated values. e.g.: arg1=val1;arg2=val2. Minimum length = 1
connectionkeepalive	<String>	Read-write	If enabled, Citrix ADC keeps the ICAP connection alive after a transaction to reuse it to send next ICAP request.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: ENABLED Possible values = ENABLED, DISABLED
allow204	<String>	Read-write	Enable or Disable sending Allow: 204 header in ICAP request. Default value: ENABLED Possible values = ENABLED, DISABLED
inserticapheaders	<String>	Read-write	Insert custom ICAP headers in the ICAP request to send to ICAP server. The headers can be static or can be dynamically constructed using PI Policy Expression. For example, to send static user agent and Client's IP address, the expression can be specified as "User-Agent: NS-ICAP-Client/ V1.0\r\nX-Client-IP: "+CLIENT.IP.SRC+"\r \n". The Citrix ADC does not check the validity of the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			specified header name-value. You must manually validate the specified header syntax. Minimum length = 1
inserthttprequest	<String>	Read-write	Exact HTTP request, in the form of an expression, which the Citrix ADC encapsulates and sends to the ICAP server. If you set this parameter, the ICAP request is sent using only this header. This can be used when the HTTP header is not available to send or ICAP server only needs part of the incoming HTTP request. The request expression is constrained by the feature for which it is used. The Citrix ADC does not check the validity of this request. You must manually validate the request. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
reqtimeout	<Integer>	Read-write	Time, in seconds, within which the remote server should respond to the ICAP-request. If the Netscaler does not receive full response with this time, the specified request timeout action is performed. Zero value disables this timeout functionality. Default value: 0 Minimum value = 0 Maximum value = 86400
reqtimeoutaction	<String>	Read-write	Name of the action to perform if the Vserver/Server representing the remote service does not respond with any response within the timeout value configured. The Supported actions are * BYPASS - This Ignores the remote server response and sends the request/response to Client/Server.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			* If the ICAP response with Encapsulated headers is not received within the request-timeout value configured, this Ignores the remote ICAP server response and sends the Full request/ response to Server/ Client. * RESET - Reset the client connection by closing it. The client program, such as a browser, will handle this and may inform the user. The client may then resend the request if desired. * DROP - Drop the request without sending a response to the user. Default value: RESET Possible values = BYPASS, DROP, RESET

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
logaction	<String>	Read-write	Name of the audit message action which would be evaluated on receiving the ICAP response to emit the logs.
inspecthttp2	<String>	Read-write	Enable or Disable ICAP inspection for HTTP/2 traffic. Default value: DISABLED Possible values = ENABLED, DISABLED
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsicapprofile **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nsicapprofile":{

<b>"name":<String_value>,

</b>"preview":<String_value>,

"previewlength":<Integer_value>,
```

```
<b>"uri":<String_value>,

</b>"hostheader":<String_value>,

"useragent":<String_value>,

<b>"mode":<String_value>,

</b>"queryparams":<String_value>,

"connectionkeepalive":<String_value>,

"allow204":<String_value>,

"inserticapheaders":<String_value>,

"inserthttprequest":<String_value>,

"reqtimeout":<Integer_value>,

"reqtimeoutaction":<String_value>,

"logaction":<String_value>,

"inspecthttp2":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsicapprofile/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsicapprofile **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nsicapprofile":{

<b>"name":<String_value>,

</b>"preview":<String_value>,

"previewlength":<Integer_value>,

"uri":<String_value>,

"hostheader":<String_value>,

"useragent":<String_value>,

"mode":<String_value>,

"queryparams":<String_value>,

"connectionkeepalive":<String_value>,

"allow204":<String_value>,

"inserticapheaders":<String_value>,

"inserthttprequest":<String_value>,

"reqtimeout":<Integer_value>,

"reqtimeoutaction":<String_value>,
```

```
"logaction":<String_value>,

"inspecthttp2":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsicapprofile? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nsicapprofile":{

<b>"name":<String_value>,

</b>"preview":true,

"previewlength":true,

"hostheader":true,

"useragent":true,

"queryparams":true,

"connectionkeepalive":true,

"allow204":true,
```

```
"inserticapheaders":true,

"inserthttprequest":true,

"reqtimeout":true,

"reqtimeoutaction":true,

"logaction":true,

"inspecthttp2":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsicapprofile **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/nsicapprofile? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/nsicapprofile? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of nsicapprofile resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/nsicapprofile? **view=summary**

Use this query-parameter to get the summary output of nsicapprofile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/nsicapprofile? **pagesize=#no;pageno=#no**

Use this query-parameter to get the nsicapprofile resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nsicapprofile": [ {

"name":<String_value>,

"preview":<String_value>,

"previewlength":<Integer_value>,

"uri":<String_value>,

"hostheader":<String_value>,

"useragent":<String_value>,

"mode":<String_value>,

"queryparams":<String_value>,

"connectionkeepalive":<String_value>,

"allow204":<String_value>,

"inserticapheaders":<String_value>,

"inserthttprequest":<String_value>,
```

```
"reqtimeout":<Integer_value>,

"reqtimeoutaction":<String_value>,

"logaction":<String_value>,

"inspecthttp2":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsicapprofile/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/nsicapprofile/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/nsicapprofile/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of nsicapprofile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "nsicapprofile": [ {

"name":<String_value>,

"preview":<String_value>,

"previewlength":<Integer_value>,

"uri":<String_value>,

"hostheader":<String_value>,

"useragent":<String_value>,

"mode":<String_value>,

"queryparams":<String_value>,

"connectionkeepalive":<String_value>,

"allow204":<String_value>,

"inserticapheaders":<String_value>,

"inserthttprequest":<String_value>,

"reqtimeout":<Integer_value>,

"reqtimeoutaction":<String_value>,

"logaction":<String_value>,

"inspecthttp2":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsicapprofile? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nsicapprofile": [ { "__count": "#no"} ] }
```

nsip

Configuration for ip resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ipaddress	<String>	Read-write	IPv4 address to create on the Citrix ADC. Cannot be changed after the IP address is created. Minimum length = 1
netmask	<String>	Read-write	Subnet mask associated with the IP address.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
type	<String>	Read-write	Type of the IP address to create on the Citrix ADC. Cannot be changed after the IP address is created. The following are the different types of Citrix ADC owned IP addresses: * A Subnet IP (SNIP) address is used by the Citrix ADC to communicate with the servers. The Citrix ADC also uses the subnet IP address when generating its own packets, such as packets related to dynamic routing protocols, or to send monitor probes to check the health of the servers. * A Virtual IP (VIP) address is the IP address associated with a virtual server. It is the IP address to which clients connect. An appliance managing

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			a wide range of traffic may have many VIPs configured. Some of the attributes of the VIP address are customized to meet the requirements of the virtual server. * A GSLB site IP (GSLBIP) address is associated with a GSLB site. It is not mandatory to specify a GSLBIP address when you initially configure the Citrix ADC. A GSLBIP address is used only when you create a GSLB site. * A Cluster IP (CLIP) address is the management address of the cluster. All cluster configurations must be performed by accessing the cluster through this IP address. Default value: SNIP

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = SNIP, VIP, NSIP, HostIP, GSLBsiteIP, CLIP
arp	<String>	Read-write	Respond to ARP requests for this IP address. Default value: ENABLED Possible values = ENABLED, DISABLED
icmp	<String>	Read-write	Respond to ICMP requests for this IP address. Default value: ENABLED Possible values = ENABLED, DISABLED
vserver	<String>	Read-write	Use this option to set (enable or disable) the virtual server attribute for this IP address. Default value: ENABLED Possible values = ENABLED, DISABLED
telnet	<String>	Read-write	Allow Telnet access to this IP address.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: ENABLED Possible values = ENABLED, DISABLED
ftp	<String>	Read-write	Allow File Transfer Protocol (FTP) access to this IP address. Default value: ENABLED Possible values = ENABLED, DISABLED
gui	<String>	Read-write	Allow graphical user interface (GUI) access to this IP address. Default value: ENABLED Possible values = ENABLED, SECUREONLY, DISABLED
ssh	<String>	Read-write	Allow secure shell (SSH) access to this IP address. Default value: ENABLED Possible values = ENABLED, DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
snmp	<String>	Read-write	Allow Simple Network Management Protocol (SNMP) access to this IP address. Default value: ENABLED Possible values = ENABLED, DISABLED
mgmtaccess	<String>	Read-write	Allow access to management applications on this IP address. Default value: DISABLED Possible values = ENABLED, DISABLED
restrictaccess	<String>	Read-write	Block access to nonmanagement applications on this IP. This option is applicable for MIPs, SNIPs, and NSIP, and is disabled by default. Nonmanagement applications can run on the underlying Citrix ADC Free BSD operating system. Default value: DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ENABLED, DISABLED
dynamicrouting	<String>	Read-write	Allow dynamic routing on this IP address. Specific to Subnet IP (SNIP) address. Default value: DISABLED Possible values = ENABLED, DISABLED
decrementttl	<String>	Read-write	Decrement TTL by 1 when ENABLED.This setting is applicable only for UDP traffic. Default value: DISABLED Possible values = ENABLED, DISABLED
ospf	<String>	Read-write	Use this option to enable or disable OSPF on this IP address for the entity. Default value: DISABLED Possible values = ENABLED, DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
bgp	<String>	Read-write	Use this option to enable or disable BGP on this IP address for the entity. Default value: DISABLED Possible values = ENABLED, DISABLED
rip	<String>	Read-write	Use this option to enable or disable RIP on this IP address for the entity. Default value: DISABLED Possible values = ENABLED, DISABLED
hostroute	<String>	Read-write	Option to push the VIP to ZebOS routing table for Kernel route redistribution through dynamic routing protocols. Possible values = ENABLED, DISABLED
advertiseondefaultpartition	<String>	Read-write	Advertise VIPs from Shared VLAN on Default Partition.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: DISABLED Possible values = ENABLED, DISABLED
networkroute	<String>	Read-write	Option to push the SNIP subnet to ZebOS routing table for Kernel route redistribution through dynamic routing protocol. Possible values = ENABLED, DISABLED
tag	<Integer>	Read-write	Tag value for the network/host route associated with this IP. Default value: 0
hostrtgw	<String>	Read-write	IP address of the gateway of the route for this VIP address. Default value: -1
metric	<Integer>	Read-write	Integer value to add to or subtract from the cost of the route advertised for the VIP address. Minimum value = -16777215
vserverrhilevel	<String>	Read-write	Advertise the route for the Virtual IP (VIP) address on the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			basis of the state of the virtual servers associated with that VIP. * NONE - Advertise the route for the VIP address, regardless of the state of the virtual servers associated with the address. * ONE VSERVER - Advertise the route for the VIP address if at least one of the associated virtual servers is in UP state. * ALL VSERVER - Advertise the route for the VIP address if all of the associated virtual servers are in UP state. * VSVR_CNTRLD - Advertise the route for the VIP address according to the RHIstate (RHI STATE) parameter setting on all the associated virtual servers of the VIP

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			address along with their states. When Vserver RHI Level (RHI) parameter is set to VSVR_CNTRLD, the following are different RHI behaviors for the VIP address on the basis of RHIstate (RHI STATE) settings on the virtual servers associated with the VIP address: * If you set RHI STATE to PASSIVE on all virtual servers, the Citrix ADC always advertises the route for the VIP address. * If you set RHI STATE to ACTIVE on all virtual servers, the Citrix ADC advertises the route for the VIP address if at least one of the associated virtual

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			servers is in UP state. *If you set RHI STATE to ACTIVE on some and PASSIVE on others, the Citrix ADC advertises the route for the VIP address if at least one of the associated virtual servers, whose RHI STATE set to ACTIVE, is in UP state. Default value: ONE_VSERVER Possible values = ONE_VSERVER, ALL_VSERVERS, NONE, VSVR_CNTRLD
ospflsatype	<String>	Read-write	Type of LSAs to be used by the OSPF protocol, running on the Citrix ADC, for advertising the route for this VIP address. Default value: TYPE5 Possible values = TYPE1, TYPE5

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ospfarea	<Integer>	Read-write	ID of the area in which the type1 link-state advertisements (LSAs) are to be advertised for this virtual IP (VIP) address by the OSPF protocol running on the Citrix ADC. When this parameter is not set, the VIP is advertised on all areas. Default value: -1 Minimum value = 0 Maximum value = 4294967294LU
state	<String>	Read-write	Enable or disable the IP address. Default value: ENABLED Possible values = ENABLED, DISABLED
vrid	<Integer>	Read-write	A positive integer that uniquely identifies a VMAC address for binding to this VIP address. This binding is used to set up Citrix ADCs in an active-active configuration using VRRP.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum value = 1 Maximum value = 255
icmpresponse	<String>	Read-write	Respond to ICMP requests for a Virtual IP (VIP) address on the basis of the states of the virtual servers associated with that VIP. Available settings function as follows: * NONE - The Citrix ADC responds to any ICMP request for the VIP address, irrespective of the states of the virtual servers associated with the address. * ONE VSERVER - The Citrix ADC responds to any ICMP request for the VIP address if at least one of the associated virtual servers is in UP state. * ALL VSERVER - The Citrix ADC responds to any ICMP request for the VIP address if

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			all of the associated virtual servers are in UP state. * VSVR_CNTRLD - The behavior depends on the ICMP VSERVER RESPONSE setting on all the associated virtual servers. The following settings can be made for the ICMP VSERVER RESPONSE parameter on a virtual server: * If you set ICMP VSERVER RESPONSE to PASSIVE on all virtual servers, Citrix ADC always responds. * If you set ICMP VSERVER RESPONSE to ACTIVE on all virtual servers, Citrix ADC responds

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			if even one virtual server is UP. * When you set ICMP VSERVER RESPONSE to ACTIVE on some and PASSIVE on others, Citrix ADC responds if even one virtual server set to ACTIVE is UP. Default value: 5 Possible values = NONE, ONE_VSERVER, ALL_VSERVERS, VSVR_CNTRLD
ownernode	<Integer>	Read-write	The owner node in a Cluster for this IP address. Owner node can vary from 0 to 31. If ownernode is not specified then the IP is treated as Striped IP. Default value: 255
arpresponse	<String>	Read-write	Respond to ARP requests for a Virtual IP (VIP) address on the basis of the states of the virtual servers associated with that VIP.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Available settings function as follows: * NONE - The Citrix ADC responds to any ARP request for the VIP address, irrespective of the states of the virtual servers associated with the address. * ONE VSERVER - The Citrix ADC responds to any ARP request for the VIP address if at least one of the associated virtual servers is in UP state. * ALL VSERVER - The Citrix ADC responds to any ARP request for the VIP address if all of the associated virtual servers are in UP state. Default value: 5 Possible values = NONE, ONE_VSERVER, ALL_VSERVERS

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ownerdownresponse	<String>	Read-write	in cluster system, if the owner node is down, whether should it respond to icmp/arp. Default value: YES Possible values = YES, NO
td	<Integer>	Read-write	Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0. TD id 4095 is used reserved for LSN use . Minimum value = 0 Maximum value = 4095
arpowner	<Integer>	Read-write	The arp owner in a Cluster for this IP address. It can vary from 0 to 31. Default value: 255
mptcpadvertise	<String>	Read-write	If enabled, this IP will be advertised by Citrix ADC to MPTCP enabled

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			clients as part of ADD_ADDR option. Default value: NO Possible values = YES, NO
flags	<Integer>	Read-only	The flags for this entry.
hostrtgwact	<String>	Read-only	Actual Gateway used for advertising host route.
ospfareaval	<Integer>	Read-only	The area ID of the area in which OSPF Type1 LSAs are advertised.
viprtadv2bsd	<Boolean>	Read-only	Whether this route is advertised to FreeBSD.
vipvsercount	<Integer>	Read-only	Number of vservers bound to this VIP.
vipvserdowncount	<Integer>	Read-only	Number of vservers bound to this VIP, which are down.
vipvsrvrrhiactivecoun t	<Integer>	Read-only	Number of vservers that have RHI state ACTIVE.
vipvsrvrrhiactiveupco unt	<Integer>	Read-only	Number of vservers that have RHI state ACTIVE, which are UP.
freeports	<Integer>	Read-only	Number of free Ports available on this IP.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
iptype	<String[]>	Read-only	. Possible values = SNIP, VIP, NSIP, HostIP, GSLBsiteIP, CLIP
operationalarpowner	<Integer>	Read-only	Run time operational Arp Owner.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- ENABLE
- DISABLE
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsip **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nsip":{

<b>"ipaddress":<String_value>,

</b><b>"netmask":<String_value>,

</b>"type":<String_value>,

"arp":<String_value>,

"icmp":<String_value>,

"vserver":<String_value>,

"telnet":<String_value>,
```

```
"ftp":<String_value>,

"gui":<String_value>,

"ssh":<String_value>,

"snmp":<String_value>,

"mgmtaccess":<String_value>,

"restrictaccess":<String_value>,

"dynamicrouting":<String_value>,

"decrementttl":<String_value>,

"ospf":<String_value>,

"bgp":<String_value>,

"rip":<String_value>,

"hostroute":<String_value>,

"advertiseondefaultpartition":<String_value>,

"networkroute":<String_value>,

"tag":<Integer_value>,

"hostrtgw":<String_value>,

"metric":<Integer_value>,

"vserverrhilevel":<String_value>,

"ospflsatype":<String_value>,

"ospfarea":<Integer_value>,

"state":<String_value>,

"vrid":<Integer_value>,
```

```
"icmpresponse":<String_value>,

"ownernode":<Integer_value>,

"arpresponse":<String_value>,

"ownerdownresponse":<String_value>,

"td":<Integer_value>,

"arpowner":<Integer_value>,

"mptcpadvertise":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsip/ ipaddress_value<String> **Query-parameters: args=td: <Integer_value>**
update
URL: http:// <netscaler-ip-address> /nitro/v1/config/nsip **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nsip":{

<b>"ipaddress":<String_value>,

</b>"td":<Integer_value>,
```

```
"netmask":<String_value>,

"arp":<String_value>,

"icmp":<String_value>,

"vserver":<String_value>,

"telnet":<String_value>,

"ftp":<String_value>,

"gui":<String_value>,

"ssh":<String_value>,

"snmp":<String_value>,

"mgmtaccess":<String_value>,

"restrictaccess":<String_value>,

"decrementttl":<String_value>,

"dynamicrouting":<String_value>,

"ospf":<String_value>,

"bgp":<String_value>,

"rip":<String_value>,

"hostroute":<String_value>,

"advertiseondefaultpartition":<String_value>,

"networkroute":<String_value>,

"hostrtgw":<String_value>,

"metric":<Integer_value>,

"vserverrhilevel":<String_value>,
```

```
"ospflsatype":<String_value>,

"ospfarea":<Integer_value>,

"tag":<Integer_value>,

"vrid":<Integer_value>,

"icmpresponse":<String_value>,

"arpresponse":<String_value>,

"ownerdownresponse":<String_value>,

"arpowner":<Integer_value>,

"mptcpadvertise":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

unset

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsip? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nsip":{

<b>"ipaddress":<String_value>,

</b>"td":<Integer_value>,
```

```
"ospfarea":true,

"hostrtgw":true,

"netmask":true,

"arp":true,

"icmp":true,

"vserver":true,

"telnet":true,

"ftp":true,

"gui":true,

"ssh":true,

"snmp":true,

"mgmtaccess":true,

"restrictaccess":true,

"decrementttl":true,

"dynamicrouting":true,

"ospf":true,

"bgp":true,

"rip":true,

"hostroute":true,

"advertiseondefaultpartition":true,

"networkroute":true,

"metric":true,
```

```
"vserverrhilevel":true,

"ospflsatype":true,

"tag":true,

"vrid":true,

"icmpresponse":true,

"arpresponse":true,

"ownerdownresponse":true,

"arpowner":true,

"mptcpadvertise":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

enable

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsip? **action=enable HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nsip":{

<b>"ipaddress":<String_value>,

</b>"td":<Integer_value>
```

```
}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

disable

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsip? **action=disable HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nsip":{

<b>"ipaddress":<String_value>,

</b>"td":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

get (all)

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsip **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/nsip? **args=ipaddress: <String_value> ,td: <Integer_value> ,type: <String_value>**

Use this query-parameter to get nsip resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/config/nsip? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/nsip? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of nsip resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/nsip? **view=summary**

Use this query-parameter to get the summary output of nsip resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/nsip? **pagesize=#no;pageno=#no**

Use this query-parameter to get the nsip resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nsip": [ {

ipaddress:<String_value>,td:<Integer_value>,type:<String_value>"netmask":<
String_value>,

"flags":<Integer_value>,

"arp":<String_value>,

"icmp":<String_value>,
```

```
"vserver":<String_value>,

"telnet":<String_value>,

"ssh":<String_value>,

"gui":<String_value>,

"snmp":<String_value>,

"ftp":<String_value>,

"mgmtaccess":<String_value>,

"restrictaccess":<String_value>,

"decrementttl":<String_value>,

"dynamicrouting":<String_value>,

"bgp":<String_value>,

"ospf":<String_value>,

"rip":<String_value>,

"hostroute":<String_value>,

"advertiseondefaultpartition":<String_value>,

"networkroute":<String_value>,

"tag":<Integer_value>,

"hostrtgw":<String_value>,

"hostrtgwact":<String_value>,

"metric":<Integer_value>,

"ospfarea":<Integer_value>,

"ospfareaval":<Integer_value>,
```

```
"vserverrhilevel":<String_value>,

"viprtadv2bsd":<Boolean_value>,

"vipvsercount":<Integer_value>,

"vipvserdowncount":<Integer_value>,

"vipvsrvrrhiactivecount":<Integer_value>,

"vipvsrvrrhiactiveupcount":<Integer_value>,

"ospflsatype":<String_value>,

"state":<String_value>,

"freeports":<Integer_value>,

"vrid":<Integer_value>,

"iptype":<String[]_value>,

"icmpresponse":<String_value>,

"ownernode":<Integer_value>,

"arpresponse":<String_value>,

"ownerdownresponse":<String_value>,

"arpowner":<Integer_value>,

"operationalarpowner":<Integer_value>,

"mptcpadvertise":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

count

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsip? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nsip": [ { "__count": "#no"} ] }
```

nsip6

Configuration for ip6 resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ipv6address	<String>	Read-write	IPv6 address to create on the Citrix ADC. Minimum length = 1
scope	<String>	Read-write	Scope of the IPv6 address to be created. Cannot be changed after the IP address is created.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: global Possible values = global, link-local
type	<String>	Read-write	Type of IP address to be created on the Citrix ADC. Cannot be changed after the IP address is created. Default value: SNIP Possible values = NSIP, VIP, SNIP, GSLBsiteIP, ADNSsvcIP, RADIUSListenersvcIP, CLIP
vlan	<Integer>	Read-write	The VLAN number. Default value: 0 Minimum value = 0 Maximum value = 4094
nd	<String>	Read-write	Respond to Neighbor Discovery (ND) requests for this IP address. Default value: ENABLED Possible values = ENABLED, DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
icmp	<String>	Read-write	Respond to ICMP requests for this IP address. Default value: ENABLED Possible values = ENABLED, DISABLED
vserver	<String>	Read-write	Enable or disable the state of all the virtual servers associated with this VIP6 address. Default value: ENABLED Possible values = ENABLED, DISABLED
telnet	<String>	Read-write	Allow Telnet access to this IP address. Default value: ENABLED Possible values = ENABLED, DISABLED
ftp	<String>	Read-write	Allow File Transfer Protocol (FTP) access to this IP address. Default value: ENABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ENABLED, DISABLED
gui	<String>	Read-write	Allow graphical user interface (GUI) access to this IP address. Default value: ENABLED Possible values = ENABLED, SECUREONLY, DISABLED
ssh	<String>	Read-write	Allow secure Shell (SSH) access to this IP address. Default value: ENABLED Possible values = ENABLED, DISABLED
snmp	<String>	Read-write	Allow Simple Network Management Protocol (SNMP) access to this IP address. Default value: ENABLED Possible values = ENABLED, DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
mgmtaccess	<String>	Read-write	Allow access to management applications on this IP address. Default value: DISABLED Possible values = ENABLED, DISABLED
restrictaccess	<String>	Read-write	Block access to nonmanagement applications on this IP address. This option is applicable forMIP6s, SNIP6s, and NSIP6s, and is disabled by default. Nonmanagement applications can run on the underlying Citrix ADC Free BSD operating system. Default value: DISABLED Possible values = ENABLED, DISABLED
dynamicrouting	<String>	Read-write	Allow dynamic routing on this IP address. Specific to Subnet IPv6 (SNIP6) address. Default value: DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ENABLED, DISABLED
decrementhoplimit	<String>	Read-write	Decrement Hop Limit by 1 when ENABLED.This setting is applicable only for UDP traffic. Default value: DISABLED Possible values = ENABLED, DISABLED
hostroute	<String>	Read-write	Option to push the VIP6 to ZebOS routing table for Kernel route redistribution through dynamic routing protocols. Possible values = ENABLED, DISABLED
advertiseondefaultpartition	<String>	Read-write	Advertise VIPs from Shared VLAN on Default Partition. Default value: DISABLED Possible values = ENABLED, DISABLED
networkroute	<String>	Read-write	Option to push the SNIP6 subnet to ZebOS routing table

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			for Kernel route redistribution through dynamic routing protocol. Possible values = ENABLED, DISABLED
tag	<Integer>	Read-write	Tag value for the network/host route associated with this IP. Default value: 0
ip6hostrtgw	<String>	Read-write	IPv6 address of the gateway for the route. If Gateway is not set, VIP uses :: as the gateway. Default value: 0
metric	<Integer>	Read-write	Integer value to add to or subtract from the cost of the route advertised for the VIP6 address. Minimum value = -16777215
vserverrhilevel	<String>	Read-write	Advertise or do not advertise the route for the Virtual IP (VIP6) address on the basis of the state of the virtual servers associated with that VIP6. * NONE - Advertise the route for the VIP6 address,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			irrespective of the state of the virtual servers associated with the address. * ONE VSERVER - Advertise the route for the VIP6 address if at least one of the associated virtual servers is in UP state. * ALL VSERVER - Advertise the route for the VIP6 address if all of the associated virtual servers are in UP state. * VSVR_CNTRLD. Advertise the route for the VIP address according to the RHIstate (RHI STATE) parameter setting on all the associated virtual servers of the VIP address along with their states. When Vserver RHI Level (RHI) parameter is set to

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			VSVR_CNTRLD, the following are different RHI behaviors for the VIP address on the basis of RHIstate (RHI STATE) settings on the virtual servers associated with the VIP address: * If you set RHI STATE to PASSIVE on all virtual servers, the Citrix ADC always advertises the route for the VIP address. * If you set RHI STATE to ACTIVE on all virtual servers, the Citrix ADC advertises the route for the VIP address if at least one of the associated virtual servers is in UP state. *If you set RHI STATE to ACTIVE on some and PASSIVE on others, the Citrix ADC

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			advertises the route for the VIP address if at least one of the associated virtual servers, whose RHI STATE set to ACTIVE, is in UP state. Default value: ONE_VSERVER Possible values = ONE_VSERVER, ALL_VSERVERS, NONE, VSVR_CNTRLD
ospf6lsatype	<String>	Read-write	Type of LSAs to be used by the IPv6 OSPF protocol, running on the Citrix ADC, for advertising the route for the VIP6 address. Default value: EXTERNAL Possible values = INTRA_AREA, EXTERNAL
ospfarea	<Integer>	Read-write	ID of the area in which the Intra-Area-Prefix LSAs are to be advertised for the VIP6 address by the IPv6 OSPF protocol running on the Citrix

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			ADC. When ospfArea is not set, VIP6 is advertised on all areas. Default value: -1 Minimum value = 0 Maximum value = 4294967294LU
state	<String>	Read-write	Enable or disable the IP address. Default value: ENABLED Possible values = DISABLED, ENABLED
map	<String>	Read-write	Mapped IPV4 address for the IPV6 address.
vrid6	<Integer>	Read-write	A positive integer that uniquely identifies a VMAC address for binding to this VIP address. This binding is used to set up Citrix ADCs in an active-active configuration using VRRP. Minimum value = 1 Maximum value = 255
ownernode	<Integer>	Read-write	ID of the cluster node for which you

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			are adding the IP address. Must be used if you want the IP address to be active only on the specific node. Can be configured only through the cluster IP address. Cannot be changed after the IP address is created. Default value: 255
ownerdownresponse	<String>	Read-write	in cluster system, if the owner node is down, whether should it respond to icmp/arp. Default value: YES Possible values = YES, NO
td	<Integer>	Read-write	Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0. Minimum value = 0 Maximum value = 4094

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ndowner	<Integer>	Read-write	NdOwner in Cluster for VIPS and Striped SNIPS. Default value: 255
mptcpadvertise	<String>	Read-write	If enabled, this IP will be advertised by Citrix ADC to MPTCP enabled clients as part of ADD_ADDR option. Default value: NO Possible values = YES, NO
icmpresponse	<String>	Read-write	Respond to ICMPv6 requests for a Virtual IP (VIP) address on the basis of the states of the virtual servers associated with that VIP. Default value: 5 Possible values = NONE, ONE_VSERVER, ALL_VSERVERS, VSVR_CNTRLD
iptype	<String[]>	Read-only	The type of the IPv6 address. Possible values = NSIP, VIP, SNIP, GSLBsiteIP, ADNSsvcIP, RADIUSListenersvcIP, CLIP

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
curstate	<String>	Read-only	Current state of this IP. Default value: ENABLED Possible values = DISABLED, ENABLED
viprtadv2bsd	<Boolean>	Read-only	Whether this route is advertised to FreeBSD.
vipvsercount	<Integer>	Read-only	Number of vservers bound to this VIP.
vipvserdowncount	<Integer>	Read-only	Number of vservers bound to this VIP, which are down.
systemtype	<String>	Read-only	The type of the System. Possible Values: Standalone, HA, Cluster. Used for display purpose. Possible values = Stand-alone, HA, Cluster
operationalndowner	<Integer>	Read-only	Operational ND6 Owner.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD

- DELETE
- UPDATE
- UNSET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsip6 **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nsip6":{

<b>"ipv6address":<String_value>,

</b>"scope":<String_value>,

"type":<String_value>,

"vlan":<Integer_value>,

"nd":<String_value>,

"icmp":<String_value>,

"vserver":<String_value>,

"telnet":<String_value>,

"ftp":<String_value>,

"gui":<String_value>,

"ssh":<String_value>,

"snmp":<String_value>,

"mgmtaccess":<String_value>,

"restrictaccess":<String_value>,

"dynamicrouting":<String_value>,

"decrementhoplimit":<String_value>,

"hostroute":<String_value>,

"advertiseondefaultpartition":<String_value>,

"networkroute":<String_value>,

"tag":<Integer_value>,
```

```
"ip6hostrtgw":<String_value>,

"metric":<Integer_value>,

"vserverrhilevel":<String_value>,

"ospf6lsatype":<String_value>,

"ospfarea":<Integer_value>,

"state":<String_value>,

"map":<String_value>,

"vrid6":<Integer_value>,

"ownernode":<Integer_value>,

"ownerdownresponse":<String_value>,

"td":<Integer_value>,

"ndowner":<Integer_value>,

"mptcpadvertise":<String_value>,

"icmpresponse":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsip6/ ipv6address_value<String> **Query-parameters: args=td: <Integer_value>**

update

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsip6 **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nsip6":{

<b>"ipv6address":<String_value>,

</b>"td":<Integer_value>,

"nd":<String_value>,

"icmp":<String_value>,

"vserver":<String_value>,

"telnet":<String_value>,

"ftp":<String_value>,

"gui":<String_value>,

"ssh":<String_value>,

"snmp":<String_value>,

"mgmtaccess":<String_value>,

"ownerdownresponse":<String_value>,

"restrictaccess":<String_value>,

"state":<String_value>,

"map":<String_value>,

"decrementhoplimit":<String_value>,

"dynamicrouting":<String_value>,
```

```
"hostroute":<String_value>,

"advertiseondefaultpartition":<String_value>,

"networkroute":<String_value>,

"ip6hostrtgw":<String_value>,

"metric":<Integer_value>,

"vserverrhilevel":<String_value>,

"ospf6lsatype":<String_value>,

"ospfarea":<Integer_value>,

"tag":<Integer_value>,

"vrid6":<Integer_value>,

"ndowner":<Integer_value>,

"mptcpadvertise":<String_value>,

"icmpresponse":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

unset

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsip6? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nsip6":{

<b>"ipv6address":<String_value>,

</b>"td":<Integer_value>,

"ospfarea":true,

"nd":true,

"icmp":true,

"vserver":true,

"telnet":true,

"ftp":true,

"gui":true,

"ssh":true,

"snmp":true,

"mgmtaccess":true,

"ownerdownresponse":true,

"restrictaccess":true,

"state":true,

"map":true,

"decrementhoplimit":true,

"dynamicrouting":true,

"hostroute":true,

"advertiseondefaultpartition":true,

"networkroute":true,
```

```
"ip6hostrtgw":true,

"metric":true,

"vserverrhilevel":true,

"ospf6lsatype":true,

"tag":true,

"vrid6":true,

"ndowner":true,

"mptcpadvertise":true,

"icmpresponse":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error
get (all)
URL: http:// <netscaler-ip-address> /nitro/v1/config/nsip6 **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/nsip6? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/nsip6? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of nsip6 resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/nsip6? **view=summary**

Use this query-parameter to get the summary output of nsip6 resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/nsip6? **pagesize=#no;pageno=#no**

Use this query-parameter to get the nsip6 resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nsip6": [ {

"ipv6address":<String_value>,

"td":<Integer_value>,

"scope":<String_value>,

"type":<String_value>,

"iptype":<String[]_value>,

"vlan":<Integer_value>,

"nd":<String_value>,

"icmp":<String_value>,

"vserver":<String_value>,

"telnet":<String_value>,
```

```
"ssh":<String_value>,

"gui":<String_value>,

"snmp":<String_value>,

"ftp":<String_value>,

"mgmtaccess":<String_value>,

"restrictaccess":<String_value>,

"state":<String_value>,

"curstate":<String_value>,

"map":<String_value>,

"decrementhoplimit":<String_value>,

"dynamicrouting":<String_value>,

"hostroute":<String_value>,

"advertiseondefaultpartition":<String_value>,

"networkroute":<String_value>,

"tag":<Integer_value>,

"ip6hostrtgw":<String_value>,

"metric":<Integer_value>,

"vserverrhilevel":<String_value>,

"viprtadv2bsd":<Boolean_value>,

"vipvsercount":<Integer_value>,

"vipvserdowncount":<Integer_value>,

"ospf6lsatype":<String_value>,
```

```
"ospfarea":<Integer_value>,

"ownernode":<Integer_value>,

"vrid6":<Integer_value>,

"ownerdownresponse":<String_value>,

"systemtype":<String_value>,

"ndowner":<Integer_value>,

"operationalndowner":<Integer_value>,

"mptcpadvertise":<String_value>,

"icmpresponse":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

count

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsip6? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nsip6": [ { "__count": "#no"} ] }
```

nsjob

Configuration for job resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
id	<Integer>	Read-write	Running job id.
name	<String>	Read-write	Running job Name.
status	<String>	Read-only	Running job status. Possible values = InProgress, Success, Failed, TimedOut
progress	<String>	Read-only	Running job progress details.
timeelapsed	<Integer>	Read-only	Number of seconds since the job started. Minimum value = 0 Maximum value = 31536000
errorcode	<Integer>	Read-only	Errcode for a particular job.
message	<String>	Read-only	Error message corresponding to the errorcode.
response	<String>	Read-only	Response of the JOB Process.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsjob **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/nsjob? **args=id: <Integer_value> ,name: <String_value>**

Use this query-parameter to get nsjob resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/config/nsjob? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/nsjob? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of nsjob resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/nsjob? **view=summary**

Use this query-parameter to get the summary output of nsjob resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/nsjob? **pagesize=#no;pageno=#no**

Use this query-parameter to get the nsjob resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nsjob": [ {

id:<Integer_value>,name:<String_value>"id":<Integer_value>,

"status":<String_value>,

"progress":<String_value>,

"timeelapsed":<Integer_value>,

"errorcode":<Integer_value>,

"message":<String_value>,

"response":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsjob/ id_value<Integer> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/nsjob/ id_value<Integer> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/nsjob/ id_value<Integer> ? **view=summary**

Use this query-parameter to get the summary output of nsjob resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "nsjob": [ {

id:<Integer_value>,name:<String_value>"id":<Integer_value>,

"status":<String_value>,

"progress":<String_value>,

"timeelapsed":<Integer_value>,

"errorcode":<Integer_value>,

"message":<String_value>,

"response":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsjob? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nsjob": [ { "__count": "#no"} ] }
```

nskeymanagerproxy

Configuration for keymanagerproxy resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
serverip	<String>	Read-write	IP address of the Key Manager proxy server. Minimum length = 1
servername	<String>	Read-write	Fully qualified domain name of the Key Manager proxy server.
port	<Integer>	Read-write	Key Manager proxy server port. Minimum value = 1025 Maximum value = 65535
nodeid	<Integer>	Read-write	Unique number that identifies the cluster node. Minimum value = 0

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum value = 31
status	<Integer>	Read-only	Status of Key Manager proxy server connectivity.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/nskeymanagerproxy **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nskeymanagerproxy":{

"serverip":<String_value>,

"servername":<String_value>,

<b>"port":<Integer_value>

</b>}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/nskeymanagerproxy/ serverip_value<String>
Query-parameters: args=servername: <String_value>
get (all)
URL: http:// <netscaler-ip-address> /nitro/v1/config/nskeymanagerproxy **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/nskeymanagerproxy? **args=serverip: <String_value> ,servername: <String_value> ,nodeid: <Integer_value>**

Use this query-parameter to get nskeymanagerproxy resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/config/nskeymanagerproxy? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/nskeymanagerproxy? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of nskeymanagerproxy resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/nskeymanagerproxy? **view=summary**

Use this query-parameter to get the summary output of nskeymanagerproxy resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/nskeymanagerproxy? **pagesize=#no;pageno=#no**

Use this query-parameter to get the nskeymanagerproxy resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nskeymanagerproxy": [ {

serverip:<String_value>,servername:<String_value>,nodeid:<Integer_value>"port":<Integer_value>,

"status":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

count

URL: http:// <netscaler-ip-address> /nitro/v1/config/nskeymanagerproxy? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nskeymanagerproxy": [ { "__count": "#no"} ] }
```

nslaslicense

Configuration for laslicense resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
filename	<String>	Read-write	Name of the file. It should not include filepath. Maximum length = 255
filelocation	<String>	Read-write	location of the file on Citrix ADC. Maximum length = 255
fixedbandwidth	<Boolean>	Read-write	apply fixed bandwidth license on ADC.
nodeid	<Integer>	Read-write	Unique number that identifies the cluster node. Minimum value = 0 Maximum value = 31
status	<String>	Read-only	Status of license activation. Default value: INACTIVE Possible values = INACTIVE, ACTIVE, EXPIRED
daystoexpiration	<Integer>	Read-only	Days to expire. Minimum value = 0 Maximum value = 4294967294
renewalprev	<Integer>	Read-only	Previous LAS renewal time.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
renewalnext	<Integer>	Read-only	Next LAS renewal time.
renewalprevdate	<String>	Read-only	Previous LAS renewal time.
renewalnextdate	<String>	Read-only	Next LAS renewal time.
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- APPLY
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

APPLY

URL: http:// <netscaler-ip-address> /nitro/v1/config/nslaslicense? **action=apply HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nslaslicense":{

<b>"filename":<String_value>,

</b><b>"filelocation":<String_value>,

</b>"fixedbandwidth":<Boolean_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/nslaslicense **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/nslaslicense? **args=nodeid: <Integer_value>**

Use this query-parameter to get nslaslicense resources based on additional properties.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nslaslicense": [ {

nodeid:<Integer_value>"status":<String_value>,

"daystoexpiration":<Integer_value>,

"renewalprev":<Integer_value>,

"renewalnext":<Integer_value>,

"renewalprevdate":<String_value>,

"renewalnextdate":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

nslicense

Configuration for license resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
wl	<Boolean>	Read-write	Web Logging.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
sp	<Boolean>	Read-write	Surge Protection.
lb	<Boolean>	Read-write	Load Balancing.
cs	<Boolean>	Read-write	Content Switching.
cr	<Boolean>	Read-write	Cache Redirect.
cmp	<Boolean>	Read-write	Compression.
delta	<Boolean>	Read-write	Delta Compression.
ssl	<Boolean>	Read-write	Secure Sockets Layer.
gslb	<Boolean>	Read-write	Global Server Load Balancing.
gslbp	<Boolean>	Read-write	GSLB Proximity.
routing	<Boolean>	Read-write	Routing.
cf	<Boolean>	Read-write	Content Filter.
contentaccelerator	<Boolean>	Read-write	transparent Integrated Caching.
ic	<Boolean>	Read-write	Integrated Caching.
sslvpn	<Boolean>	Read-write	SSL VPN.
f_sslvpn_users	<Integer>	Read-write	Number of licensed users allowed by this license.
f_ica_users	<Integer>	Read-write	Number of licensed users allowed by ICAONLY license. As long as the AG Feature is licensed,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			unlimited number of ICA connections are accepted. (In API, 0 value for this parameter means unlimited when AG license in ON).
aaa	<Boolean>	Read-write	AAA.
ospf	<Boolean>	Read-write	OSPF Routing.
rip	<Boolean>	Read-write	RIP Routing.
bgp	<Boolean>	Read-write	BGP Routing.
rewrite	<Boolean>	Read-write	Rewrite.
ipv6pt	<Boolean>	Read-write	IPv6 protocol translation.
appfw	<Boolean>	Read-write	Application Firewall.
responder	<Boolean>	Read-write	Responder.
agee	<Boolean>	Read-write	.
nsxn	<Boolean>	Read-write	.
modelid	<Integer>	Read-write	Model Number ID. Represents different numbers for two types of licenses.: * Bandwidth licenses - specifies the throughput

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			bandwidth licensed for this appliance e.g. (For 20 Gbps) Model Number ID: 20000 * vCPU licenses - specifies number of vCPUs licensed for this appliance. e.g. (For 4 vCPU) Model Number ID: 4 vCPUs.
push	<Boolean>	Read-write	Citrix ADC Push.
appflow	<Boolean>	Read-write	AppFlow.
cloudbridge	<Boolean>	Read-write	CloudBridge.
cloudbridgeappliance	<Boolean>	Read-write	.
cloudextenderappliance	<Boolean>	Read-write	.
isis	<Boolean>	Read-write	ISIS Routing.
cluster	<Boolean>	Read-write	Clustering.
ch	<Boolean>	Read-write	Call Home.
appqoe	<Boolean>	Read-write	AppQoS.
appflowica	<Boolean>	Read-write	Appflow for ICA.
isstandardlic	<Boolean>	Read-write	Standard License.
isenterpriselic	<Boolean>	Read-write	Enterprise License.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
isplatinumlic	<Boolean>	Read-write	Platinum License.
issgwylic	<Boolean>	Read-write	Simple Gateway License.
isswglic	<Boolean>	Read-write	Secure Web Gateway License.
feo	<Boolean>	Read-write	Front End Optimization.
lsn	<Boolean>	Read-write	Large Scale NAT.
licensingmode	<String>	Read-write	Pooled Licensed. Default value: Local Possible values = Local, Pooled, Fips-Pooled, CICO, Fips-CICO, EXPRESS, CPU, CPU-Local, Self Managed Pool, Self Managed vCPU, LAS, LAS (Fixed Bandwidth)
cloudsubscriptionimage	<String>	Read-write	Cloud Subscription Image. Default value: NO Possible values = YES, NO
daystoexpiration	<Integer>	Read-write	Days to expire. Minimum value = 0 Maximum value = 4294967294

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
daystolasenforcement	<Integer>	Read-write	Days to expire for lasenforcement. Minimum value = 0 Maximum value = 4294967294
rdpproxy	<Boolean>	Read-write	RDPPROXY.
rep	<Boolean>	Read-write	Reputation Services.
urlfiltering	<Boolean>	Read-write	URL Filtering.
videooptimization	<Boolean>	Read-write	Video Optimization.
forwardproxy	<Boolean>	Read-write	Forward Proxy.
sslinterception	<Boolean>	Read-write	SSL Interception.
remotecontentinspection	<Boolean>	Read-write	Remote Content Inspection.
adaptivetcp	<Boolean>	Read-write	Adaptive TCP.
cqa	<Boolean>	Read-write	Connection Quality Analytics.
bot	<Boolean>	Read-write	Bot Management.
apigateway	<Boolean>	Read-write	API Gateway.
_nextgenapiresource	<String>	Read-write	.

Operations

(click to see Properties)

- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/nslicense **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nslicense": [ {

"wl":<Boolean_value>,

"sp":<Boolean_value>,

"lb":<Boolean_value>,

"cs":<Boolean_value>,

"cr":<Boolean_value>,

"cmp":<Boolean_value>,

"delta":<Boolean_value>,

"ssl":<Boolean_value>,

"gslb":<Boolean_value>,

"gslbp":<Boolean_value>,

"routing":<Boolean_value>,

"cf":<Boolean_value>,

"contentaccelerator":<Boolean_value>,

"ic":<Boolean_value>,

"sslvpn":<Boolean_value>,

"f_sslvpn_users":<Integer_value>,

"f_ica_users":<Integer_value>,

"aaa":<Boolean_value>,

"ospf":<Boolean_value>,

"rip":<Boolean_value>,
```

```
"bgp":<Boolean_value>,

"rewrite":<Boolean_value>,

"ipv6pt":<Boolean_value>,

"appfw":<Boolean_value>,

"responder":<Boolean_value>,

"agee":<Boolean_value>,

"nsxn":<Boolean_value>,

"modelid":<Integer_value>,

"push":<Boolean_value>,

"appflow":<Boolean_value>,

"cloudbridge":<Boolean_value>,

"cloudbridgeappliance":<Boolean_value>,

"cloudextenderappliance":<Boolean_value>,

"isis":<Boolean_value>,

"cluster":<Boolean_value>,

"ch":<Boolean_value>,

"appqoe":<Boolean_value>,

"appflowica":<Boolean_value>,

"isstandardlic":<Boolean_value>,

"isenterpriselic":<Boolean_value>,

"isplatinumlic":<Boolean_value>,

"issgwylic":<Boolean_value>,
```

```
"isswglic":<Boolean_value>,

"feo":<Boolean_value>,

"lsn":<Boolean_value>,

"licensingmode":<String_value>,

"cloudsubscriptionimage":<String_value>,

"daystoexpiration":<Integer_value>,

"daystolasenforcement":<Integer_value>,

"rdpproxy":<Boolean_value>,

"rep":<Boolean_value>,

"urlfiltering":<Boolean_value>,

"videooptimization":<Boolean_value>,

"forwardproxy":<Boolean_value>,

"sslinterception":<Boolean_value>,

"remotecontentinspection":<Boolean_value>,

"adaptivetcp":<Boolean_value>,

"cqa":<Boolean_value>,

"bot":<Boolean_value>,

"apigateway":<Boolean_value>,

"_nextgenapiresource":<String_value>

}]}
```

nslicenseactivationdata

Configuration for License activation data resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
usehostname	<Boolean>	Read-write	Use hostname as identifier in licenseactivation request.
filename	<String>	Read-only	Name of the file. It should not include filepath. Maximum length = 255
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/nslicenseactivationdata **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/nslicenseactivationdata? **args=usehostname: <Boolean_value>**

Use this query-parameter to get nslicenseactivationdata resources based on additional properties.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nslicenseactivationdata": [ {

usehostname:<Boolean_value>"filename":<String_value>,

"_nextgenapiresource":<String_value>
```

```
}]}
```

nslicenseparameters

Configuration for licenseparameters resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
alert1gracetimeout	<Integer>	Read-write	If ADC remains in grace for the configured hours then first grace alert will be raised. Default value: 6 Minimum value = 0 Maximum value = 24
alert2gracetimeout	<Integer>	Read-write	If ADC remains in grace for the configured hours then major grace alert will be raised. Default value: 240 Minimum value = 24 Maximum value = 720
licenseexpiryalerttime	<Integer>	Read-write	If ADC license contract expiry date is nearer then GUI/ SNMP license expiry alert will be raised.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: 30 Minimum value = 1 Maximum value = 365
heartbeatinterval	<Integer>	Read-write	Heartbeat between ADC and Licenseserver is configurable and applicable in case of pooled licensing. Default value: 280 Minimum value = 30 Maximum value = 280
inventoryrefreshinterval	<Integer>	Read-write	Inventory refresh interval between ADC and Licenseserver is configurable and applicable in case of pooled licensing. Default value: 360 Minimum value = 45 Maximum value = 1440
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- UPDATE
- UNSET

- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/nslicenseparameters **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nslicenseparameters":{

"alert1gracetimeout":<Integer_value>,
```

```
"alert2gracetimeout":<Integer_value>,

"licenseexpiryalerttime":<Integer_value>,

"heartbeatinterval":<Integer_value>,

"inventoryrefreshinterval":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/nslicenseparameters? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nslicenseparameters":{

"alert1gracetimeout":true,

"alert2gracetimeout":true,

"licenseexpiryalerttime":true,

"heartbeatinterval":true,

"inventoryrefreshinterval":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/nslicenseparameters **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nslicenseparameters": [ {

"alert1gracetimeout":<Integer_value>,

"alert2gracetimeout":<Integer_value>,

"licenseexpiryalerttime":<Integer_value>,

"heartbeatinterval":<Integer_value>,

"inventoryrefreshinterval":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

nslicenseproxyserver

Configuration for licenseproxyserver resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
serverip	<String>	Read-write	IP address of the License proxy server. Minimum length = 1
servername	<String>	Read-write	Fully qualified domain name of the License proxy server.
port	<Integer>	Read-write	License proxy server port.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/nslicenseproxyserver **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nslicenseproxyserver":{

"serverip":<String_value>,

"servername":<String_value>,

<b>"port":<Integer_value>

</b>}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/nslicenseproxyserver/ serverip_value<String>
Query-parameters: args=servername: <String_value>
update
URL: http:// <netscaler-ip-address> /nitro/v1/config/nslicenseproxyserver **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nslicenseproxyserver":{

"serverip":<String_value>,

"servername":<String_value>,

<b>"port":<Integer_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error
get (all)
URL: http:// <netscaler-ip-address> /nitro/v1/config/nslicenseproxyserver **Query-parameters: attrs**
http:// <netscaler-ip-address> /nitro/v1/config/nslicenseproxyserver? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/nslicenseproxyserver? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of nslicenseproxyserver resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/nslicenseproxyserver? **view=summary**

Use this query-parameter to get the summary output of nslicenseproxyserver resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/nslicenseproxyserver? **pagesize=#no;pageno=#no**

Use this query-parameter to get the nslicenseproxyserver resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nslicenseproxyserver": [ {

"serverip":<String_value>,

"servername":<String_value>,

"port":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

count

URL: http:// <netscaler-ip-address> /nitro/v1/config/nslicenseproxyserver? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nslicenseproxyserver": [ { "__count": "#no"} ] }
```

nslicenseserver

Configuration for licenseserver resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
licenseserverip	<String>	Read-write	IP address of the License server. Minimum length = 1
servername	<String>	Read-write	Fully qualified domain name of the License server.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
port	<Integer>	Read-write	License server port.
forceupdateip	<Boolean>	Read-write	If this flag is used while adding the licenseserver, existing config will be overwritten. Use this flag only if you are sure that the new licenseserver has the required capacity.
licensemode	<String>	Read-write	This paramter indicates type of license customer interested while configuring add/set licenseserver. Possible values = Pooled, VCPU, CICO, SelfManagedPool, SelfManagedvCPU, LAS
username	<String>	Read-write	Username to authenticate with ADM Agent for LAS licensing. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum length = 1 Maximum length = 127
password	<String>	Read-write	Password to use when authenticating with ADM Agent for LAS licensing. Minimum length = 1
deviceprofilename	<String>	Read-write	Device profile is created on ADM and contains the user name and password of the instance(s). ADM will use this info to add the NS for registration. Minimum length = 1 Maximum length = 255
nodeid	<Integer>	Read-write	Unique number that identifies the cluster node. Minimum value = 0 Maximum value = 31
status	<Integer>	Read-only	Status of license server.
grace	<Integer>	Read-only	Grace status of server.
gptimeleft	<Integer>	Read-only	Grace time left.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
type	<String>	Read-only	License Server type CLA/ADM. Possible values = ADM, CLA
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/nslicenseserver **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nslicenseserver":{

"licenseserverip":<String_value>,

"servername":<String_value>,

"port":<Integer_value>,

"forceupdateip":<Boolean_value>,

"licensemode":<String_value>,

"username":<String_value>,

"password":<String_value>,

"deviceprofilename":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/nslicenseserver/ licenseserverip_value<String>
Query-parameters: args=servername: <String_value>
update
URL: http:// <netscaler-ip-address> /nitro/v1/config/nslicenseserver **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nslicenseserver":{

"licenseserverip":<String_value>,

"servername":<String_value>,

"port":<Integer_value>,

"licensemode":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error
get (all)
URL: http:// <netscaler-ip-address> /nitro/v1/config/nslicenseserver **Query-parameters: args**
http:// <netscaler-ip-address> /nitro/v1/config/nslicenseserver? **args=licenseserverip: <String_value> ,servername: <String_value> ,nodeid: <Integer_value>**

Use this query-parameter to get nslicenseserver resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/config/nslicenseserver? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/nslicenseserver? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of nslicenseserver resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/nslicenseserver? **view=summary**

Use this query-parameter to get the summary output of nslicenseserver resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/nslicenseserver? **pagesize=#no;pageno=#no**

Use this query-parameter to get the nslicenseserver resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nslicenseserver": [ {

licenseserverip:<String_value>,servername:<String_value>,nodeid:<Integer_value>"port":<Integer_value>,

"status":<Integer_value>,

"grace":<Integer_value>,
```

```
"gptimeleft":<Integer_value>,

"type":<String_value>,

"deviceprofilename":<String_value>,

"licensemode":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

count

URL: http:// <netscaler-ip-address> /nitro/v1/config/nslicenseserver? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nslicenseserver": [ { "__count": "#no"} ] }
```

nslicenseserverpool

Configuration for licenseserver resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
getalllicenses	<Boolean>	Read-write	If this flag is used while doing getinventory, it displays all licenses from licenseserver.
instancetotal	<Integer>	Read-only	Instance Total.
instanceavailable	<Integer>	Read-only	Instance Available.
standardbandwidthtotal	<Integer>	Read-only	Standard Bandwidth Total.
standardbandwidthavailable	<Integer>	Read-only	Standard Bandwidth Available.
enterprisebandwidthtotal	<Integer>	Read-only	Enterprise Bandwidth Total.
enterprisebandwidthavailable	<Integer>	Read-only	Enterprise Bandwidth Available.
platinumbandwidthtotal	<Integer>	Read-only	Platinum Bandwidth Total.
platinumbandwidthavailable	<Integer>	Read-only	Platinum Bandwidth Available.
standardcputotal	<Integer>	Read-only	Standard CPU Total.
standardcpuavailable	<Integer>	Read-only	Standard CPU Available.
enterprisecputotal	<Integer>	Read-only	Enterprise CPU Total.
enterprisecpuavailable	<Integer>	Read-only	Enterprise CPU Available.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
platinumcputotal	<Integer>	Read-only	Platinum CPU Total.
platinumcpuavailable	<Integer>	Read-only	Platinum CPU Available.
cpxinstancetotal	<Integer>	Read-only	CP1000 Instance Total.
cpxinstanceavailable	<Integer>	Read-only	CP1000 Instance Available.
vpx1stotal	<Integer>	Read-only	VPX1S Total.
vpx1savailable	<Integer>	Read-only	VPX1S Available.
vpx1ptotal	<Integer>	Read-only	VPX1P Total.
vpx1pavailable	<Integer>	Read-only	VPX1P Available.
vpx5stotal	<Integer>	Read-only	VPX5S Total.
vpx5savailable	<Integer>	Read-only	VPX5S Available.
vpx5ptotal	<Integer>	Read-only	VPX5P Total.
vpx5pavailable	<Integer>	Read-only	VPX5P Available.
vpx10stotal	<Integer>	Read-only	VPX10S Total.
vpx10savailable	<Integer>	Read-only	VPX10S Available.
vpx10etotal	<Integer>	Read-only	VPX10E Total.
vpx10eavailable	<Integer>	Read-only	VPX10E Available.
vpx10ptotal	<Integer>	Read-only	VPX10P Total.
vpx10pavailable	<Integer>	Read-only	VPX10P Available.
vpx25stotal	<Integer>	Read-only	VPX25S Total.
vpx25savailable	<Integer>	Read-only	VPX25S Available.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
vpx25etotal	<Integer>	Read-only	VPX25E Total.
vpx25eavailable	<Integer>	Read-only	VPX25E Available.
vpx25ptotal	<Integer>	Read-only	VPX25P Total.
vpx25pavailable	<Integer>	Read-only	VPX25P Available.
vpx50stotal	<Integer>	Read-only	VPX50S Total.
vpx50savailable	<Integer>	Read-only	VPX50S Available.
vpx50etotal	<Integer>	Read-only	VPX50E Total.
vpx50eavailable	<Integer>	Read-only	VPX50E Available.
vpx50ptotal	<Integer>	Read-only	VPX50P Total.
vpx50pavailable	<Integer>	Read-only	VPX50P Available.
vpx100stotal	<Integer>	Read-only	VPX100S Total.
vpx100savailable	<Integer>	Read-only	VPX100S Available.
vpx100etotal	<Integer>	Read-only	VPX100E Total.
vpx100eavailable	<Integer>	Read-only	VPX100E Available.
vpx100ptotal	<Integer>	Read-only	VPX100P Total.
vpx100pavailable	<Integer>	Read-only	VPX100P Available.
vpx200stotal	<Integer>	Read-only	VPX200S Total.
vpx200savailable	<Integer>	Read-only	VPX200S Available.
vpx200etotal	<Integer>	Read-only	VPX200E Total.
vpx200eavailable	<Integer>	Read-only	VPX200E Available.
vpx200ptotal	<Integer>	Read-only	VPX200P Total.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
vpx200pavailable	<Integer>	Read-only	VPX200P Available.
vpx500stotal	<Integer>	Read-only	VPX500S Total.
vpx500savailable	<Integer>	Read-only	VPX500S Available.
vpx500etotal	<Integer>	Read-only	VPX500E Total.
vpx500eavailable	<Integer>	Read-only	VPX500E Available.
vpx500ptotal	<Integer>	Read-only	VPX500P Total.
vpx500pavailable	<Integer>	Read-only	VPX500P Available.
vpx1000stotal	<Integer>	Read-only	VPX1000S Total.
vpx1000savailable	<Integer>	Read-only	VPX1000S Available.
vpx1000etotal	<Integer>	Read-only	VPX1000E Total.
vpx1000eavailable	<Integer>	Read-only	VPX1000E Available.
vpx1000ptotal	<Integer>	Read-only	VPX1000P Total.
vpx1000pavailable	<Integer>	Read-only	VPX1000P Available.
vpx2000ptotal	<Integer>	Read-only	VPX2000P Total.
vpx2000pavailable	<Integer>	Read-only	VPX2000P Available.
vpx3000stotal	<Integer>	Read-only	VPX3000S Total.
vpx3000savailable	<Integer>	Read-only	VPX3000S Available.
vpx3000etotal	<Integer>	Read-only	VPX3000E Total.
vpx3000eavailable	<Integer>	Read-only	VPX3000E Available.
vpx3000ptotal	<Integer>	Read-only	VPX3000P Total.
vpx3000pavailable	<Integer>	Read-only	VPX3000P Available.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
vpx4000ptotal	<Integer>	Read-only	VPX4000P Total.
vpx4000pavailable	<Integer>	Read-only	VPX4000P Available.
vpx5000stotal	<Integer>	Read-only	VPX5000S Total.
vpx5000savailable	<Integer>	Read-only	VPX5000S Available.
vpx5000etotal	<Integer>	Read-only	VPX5000E Total.
vpx5000eavailable	<Integer>	Read-only	VPX5000E Available.
vpx5000ptotal	<Integer>	Read-only	VPX5000P Total.
vpx5000pavailable	<Integer>	Read-only	VPX5000P Available.
vpx8000stotal	<Integer>	Read-only	VPX8000S Total.
vpx8000savailable	<Integer>	Read-only	VPX8000S Available.
vpx8000etotal	<Integer>	Read-only	VPX8000E Total.
vpx8000eavailable	<Integer>	Read-only	VPX8000E Available.
vpx8000ptotal	<Integer>	Read-only	VPX8000P Total.
vpx8000pavailable	<Integer>	Read-only	VPX8000P Available.
vpx10000stotal	<Integer>	Read-only	VPX10000S Total.
vpx10000savailable	<Integer>	Read-only	VPX10000S Available.
vpx10000etotal	<Integer>	Read-only	VPX10000E Total.
vpx10000eavailable	<Integer>	Read-only	VPX10000E Available.
vpx10000ptotal	<Integer>	Read-only	VPX10000P Total.
vpx10000pavailable	<Integer>	Read-only	VPX10000P Available.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
vpx15000stotal	<Integer>	Read-only	VPX15000S Total.
vpx15000savailable	<Integer>	Read-only	VPX15000S Available.
vpx15000etotal	<Integer>	Read-only	VPX15000E Total.
vpx15000eavailable	<Integer>	Read-only	VPX15000E Available.
vpx15000ptotal	<Integer>	Read-only	VPX15000P Total.
vpx15000pavailable	<Integer>	Read-only	VPX15000P Available.
vpx25000stotal	<Integer>	Read-only	VPX25000S Total.
vpx25000savailable	<Integer>	Read-only	VPX25000S Available.
vpx25000etotal	<Integer>	Read-only	VPX25000E Total.
vpx25000eavailable	<Integer>	Read-only	VPX25000E Available.
vpx25000ptotal	<Integer>	Read-only	VPX25000P Total.
vpx25000pavailable	<Integer>	Read-only	VPX25000P Available.
vpx40000stotal	<Integer>	Read-only	VPX40000S Total.
vpx40000savailable	<Integer>	Read-only	VPX40000S Available.
vpx40000etotal	<Integer>	Read-only	VPX40000E Total.
vpx40000eavailable	<Integer>	Read-only	VPX40000E Available.
vpx40000ptotal	<Integer>	Read-only	VPX40000P Total.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
vpx40000pavailable	<Integer>	Read-only	VPX40000P Available.
vpx100000stotal	<Integer>	Read-only	VPX100000S Total.
vpx100000savailable	<Integer>	Read-only	VPX100000S Available.
vpx100000etotal	<Integer>	Read-only	VPX100000E Total.
vpx100000eavailable	<Integer>	Read-only	VPX100000E Available.
vpx100000ptotal	<Integer>	Read-only	VPX100000P Total.
vpx100000pavailable	<Integer>	Read-only	VPX100000P Available.
licensemode	<String>	Read-only	This paramter indicates type of license customer interested while configuring add/set licenseserver. Possible values = Pooled, VCPU, CICO, SelfManagedPool, SelfManagedvCPU, LAS
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/nslicenseserverpool **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/nslicenseserverpool? **args=getalllicenses: <Boolean_value>**

Use this query-parameter to get nslicenseserverpool resources based on additional properties.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nslicenseserverpool": [ {

getalllicenses:<Boolean_value>"instancetotal":<Integer_value>,

"instanceavailable":<Integer_value>,

"standardbandwidthtotal":<Integer_value>,

"standardbandwidthavailable":<Integer_value>,

"enterprisebandwidthtotal":<Integer_value>,

"enterprisebandwidthavailable":<Integer_value>,

"platinumbandwidthtotal":<Integer_value>,

"platinumbandwidthavailable":<Integer_value>,

"standardcputotal":<Integer_value>,

"standardcpuavailable":<Integer_value>,

"enterprisecputotal":<Integer_value>,

"enterprisecpuavailable":<Integer_value>,

"platinumcputotal":<Integer_value>,

"platinumcpuavailable":<Integer_value>,

"cpxinstancetotal":<Integer_value>,

"cpxinstanceavailable":<Integer_value>,
```

```
"vpx1stotal":<Integer_value>,

"vpx1savailable":<Integer_value>,

"vpx1ptotal":<Integer_value>,

"vpx1pavailable":<Integer_value>,

"vpx5stotal":<Integer_value>,

"vpx5savailable":<Integer_value>,

"vpx5ptotal":<Integer_value>,

"vpx5pavailable":<Integer_value>,

"vpx10stotal":<Integer_value>,

"vpx10savailable":<Integer_value>,

"vpx10etotal":<Integer_value>,

"vpx10eavailable":<Integer_value>,

"vpx10ptotal":<Integer_value>,

"vpx10pavailable":<Integer_value>,

"vpx25stotal":<Integer_value>,

"vpx25savailable":<Integer_value>,

"vpx25etotal":<Integer_value>,

"vpx25eavailable":<Integer_value>,

"vpx25ptotal":<Integer_value>,

"vpx25pavailable":<Integer_value>,

"vpx50stotal":<Integer_value>,

"vpx50savailable":<Integer_value>,
```

```
"vpx50etotal":<Integer_value>,

"vpx50eavailable":<Integer_value>,

"vpx50ptotal":<Integer_value>,

"vpx50pavailable":<Integer_value>,

"vpx100stotal":<Integer_value>,

"vpx100savailable":<Integer_value>,

"vpx100etotal":<Integer_value>,

"vpx100eavailable":<Integer_value>,

"vpx100ptotal":<Integer_value>,

"vpx100pavailable":<Integer_value>,

"vpx200stotal":<Integer_value>,

"vpx200savailable":<Integer_value>,

"vpx200etotal":<Integer_value>,

"vpx200eavailable":<Integer_value>,

"vpx200ptotal":<Integer_value>,

"vpx200pavailable":<Integer_value>,

"vpx500stotal":<Integer_value>,

"vpx500savailable":<Integer_value>,

"vpx500etotal":<Integer_value>,

"vpx500eavailable":<Integer_value>,

"vpx500ptotal":<Integer_value>,

"vpx500pavailable":<Integer_value>,
```

```
"vpx1000stotal":<Integer_value>,

"vpx1000savailable":<Integer_value>,

"vpx1000etotal":<Integer_value>,

"vpx1000eavailable":<Integer_value>,

"vpx1000ptotal":<Integer_value>,

"vpx1000pavailable":<Integer_value>,

"vpx2000ptotal":<Integer_value>,

"vpx2000pavailable":<Integer_value>,

"vpx3000stotal":<Integer_value>,

"vpx3000savailable":<Integer_value>,

"vpx3000etotal":<Integer_value>,

"vpx3000eavailable":<Integer_value>,

"vpx3000ptotal":<Integer_value>,

"vpx3000pavailable":<Integer_value>,

"vpx4000ptotal":<Integer_value>,

"vpx4000pavailable":<Integer_value>,

"vpx5000stotal":<Integer_value>,

"vpx5000savailable":<Integer_value>,

"vpx5000etotal":<Integer_value>,

"vpx5000eavailable":<Integer_value>,

"vpx5000ptotal":<Integer_value>,

"vpx5000pavailable":<Integer_value>,
```

```
"vpx8000stotal":<Integer_value>,

"vpx8000savailable":<Integer_value>,

"vpx8000etotal":<Integer_value>,

"vpx8000eavailable":<Integer_value>,

"vpx8000ptotal":<Integer_value>,

"vpx8000pavailable":<Integer_value>,

"vpx10000stotal":<Integer_value>,

"vpx10000savailable":<Integer_value>,

"vpx10000etotal":<Integer_value>,

"vpx10000eavailable":<Integer_value>,

"vpx10000ptotal":<Integer_value>,

"vpx10000pavailable":<Integer_value>,

"vpx15000stotal":<Integer_value>,

"vpx15000savailable":<Integer_value>,

"vpx15000etotal":<Integer_value>,

"vpx15000eavailable":<Integer_value>,

"vpx15000ptotal":<Integer_value>,

"vpx15000pavailable":<Integer_value>,

"vpx25000stotal":<Integer_value>,

"vpx25000savailable":<Integer_value>,

"vpx25000etotal":<Integer_value>,

"vpx25000eavailable":<Integer_value>,
```

```
"vpx25000ptotal":<Integer_value>,

"vpx25000pavailable":<Integer_value>,

"vpx40000stotal":<Integer_value>,

"vpx40000savailable":<Integer_value>,

"vpx40000etotal":<Integer_value>,

"vpx40000eavailable":<Integer_value>,

"vpx40000ptotal":<Integer_value>,

"vpx40000pavailable":<Integer_value>,

"vpx100000stotal":<Integer_value>,

"vpx100000savailable":<Integer_value>,

"vpx100000etotal":<Integer_value>,

"vpx100000eavailable":<Integer_value>,

"vpx100000ptotal":<Integer_value>,

"vpx100000pavailable":<Integer_value>,

"licensemode":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

nslimitidentifier

Configuration for limit Identifier resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
limitidentifier	<String>	Read-write	Name for a rate limit identifier. Must begin with an ASCII letter or underscore (_) character, and must consist only of ASCII alphanumeric or underscore characters. Reserved words must not be used.
threshold	<Integer>	Read-write	Maximum number of requests that are allowed in the given timeslice when requests (mode is set as REQUEST_RATE) are tracked per timeslice. When connections (mode is set as CONNECTION) are tracked, it is the total number of connections that would be let through. Maximum number of tokens that are allowed in the given timeslice when Tokens (mode is set to TOKEN_RATE) are tracked per timeslice.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: 1 Minimum value = 1
timeslice	<Integer>	Read-write	Time interval, in milliseconds, specified in multiples of 10, during which requests/tokens are tracked to check if they cross the threshold. This argument is needed only when the mode is set to REQUEST_RATE or TOKEN_RATE. Default value: 1000 Minimum value = 10
mode	<String>	Read-write	Defines the type of traffic to be tracked. * REQUEST_RATE - Tracks requests/ timeslice. * CONNECTION - Tracks active transactions. * TOKEN_RATE - Tracks total input+output tokens/minute for LLM chat completions, Timeslice is fixed at 60000 ms, Useful on applications

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			serving LLM services. Examples 1. To permit 20 requests in 10 ms and 2 traps in 10 ms: add limitidentifier limit_req -mode request_rate -limitType smooth -timeslice 1000 -Threshold 2000 -trapsInTimeSlice 200 2. To permit 50 requests in 10 ms: set limitidentifier limit_req -mode request_rate -timeslice 1000 -Threshold 5000 -limitType smooth 3. To permit 1 request in 40 ms: set limitidentifier limit_req -mode request_rate -timeslice 2000 -Threshold 50 -limitType smooth

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			4. To permit 1 request in 200 ms and 1 trap in 130 ms: set limitidentifier limit_req -mode request_rate -timeslice 1000 -Threshold 5 -limitType smooth -trapsInTimeSlice 8 5. To permit 5000 requests in 1000 ms and 200 traps in 1000 ms and 20 appflow alerts in 1000ms: set limitidentifier limit_req -mode request_rate -timeslice 1000 -Threshold 5000 -limitType BURSTY -trapsInTimeSlice 200 -alertsInTimeSlice 20 6. To permit 100000 tokens in 60000 ms and 100 appflow alerts in 60000ms:

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			set limitidentifier limit_tokens -mode token_rate -timeSlice 60000 -Threshold 100000 -limittype BURSTY -alertsInTimeSlice 100. Default value: REQUEST_RATE Possible values = CONNECTION, REQUEST_RATE, TOKEN_RATE, NONE
limittype	<String>	Read-write	Smooth or bursty request type. * SMOOTH - When you want the permitted number of requests in a given interval of time to be spread evenly across the timeslice * BURSTY - When you want the permitted number of requests to exhaust the quota anytime within the timeslice. This argument is needed only when

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			the mode is set to REQUEST_RATE. Mode TOKEN_RATE only supports BURSTY type. Default value: BURSTY Possible values = BURSTY, SMOOTH
selectorname	<String>	Read-write	Name of the rate limit selector. If this argument is NULL, rate limiting will be applied on all traffic received by the virtual server or the Citrix ADC (depending on whether the limit identifier is bound to a virtual server or globally) without any filtering. Minimum length = 1
maxbandwidth	<Integer>	Read-write	Maximum bandwidth permitted, in kbps. Minimum value = 0 Maximum value = 4294967287
trapsintimeslice	<Integer>	Read-write	Number of traps to be sent in the timeslice configured. A value of 0 indicates

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			that traps are disabled. Minimum value = 0 Maximum value = 65535
alertsintimeslice	<Integer>	Read-write	Number of appflow alerts to be sent in the timeslice configured. A value of 0 indicates that alerts are disabled. A value of 65535 indicates no limit on number of appflow alerts. Default value: 65535 Minimum value = 0 Maximum value = 65535
timealign	<String>	Read-write	Value MINUTE will align the time windows for a configured timeslice to Minute boundary. TimeSlice values should be integrals of 60000ms when value MINUTE is choosen. Default : NONE, timeslice alignments will happen with next 10ms.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: NONE Possible values = NONE, MINUTE
ngname	<String>	Read-only	Nodegroup name to which this identifier belongs to.
hits	<Integer>	Read-only	The number of times this identifier was evaluated.
drop	<Integer>	Read-only	The number of times action was taken.
rule	<String[]>	Read-only	Rule.
time	<Integer>	Read-only	Time interval considered for rate limiting.
total	<Integer>	Read-only	Maximum number of requests permitted in the computed timeslice.
trapscomputedintimeslice	<Integer>	Read-only	The number of traps that would be sent in the timeslice configured. .
computedtraptimeslice	<Integer>	Read-only	The time interval computed for sending traps.
alertscomputedintimeslice	<Integer>	Read-only	The number of appflow alerts that would be sent in the timeslice configured.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
computedalerttimeslice	<Integer>	Read-only	The time interval computed for sending appflow alerts.
referencecount	<Integer>	Read-only	Total number of transactions pointing to this entry.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.
- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of

creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/nslimitidentifier **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nslimitidentifier":{

<b>"limitidentifier":<String_value>,

</b>"threshold":<Integer_value>,

"timeslice":<Integer_value>,

"mode":<String_value>,

"limittype":<String_value>,

"selectorname":<String_value>,

"maxbandwidth":<Integer_value>,

"trapsintimeslice":<Integer_value>,
```

```
"alertsintimeslice":<Integer_value>,

"timealign":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/nslimitidentifier/ limitidentifier_value<String>
HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/nslimitidentifier **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nslimitidentifier":{

<b>"limitidentifier":<String_value>,

</b>"threshold":<Integer_value>,

"timeslice":<Integer_value>,
```

```
"mode":<String_value>,

"limittype":<String_value>,

"selectorname":<String_value>,

"maxbandwidth":<Integer_value>,

"trapsintimeslice":<Integer_value>,

"alertsintimeslice":<Integer_value>,

"timealign":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/nslimitidentifier? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nslimitidentifier":{

<b>"limitidentifier":<String_value>,

</b>"selectorname":true,

"threshold":true,
```

```
"timeslice":true,

"mode":true,

"limittype":true,

"maxbandwidth":true,

"trapsintimeslice":true,

"alertsintimeslice":true,

"timealign":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/nslimitidentifier **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/nslimitidentifier? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/nslimitidentifier? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of nslimitidentifier resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/nslimitidentifier? **view=summary**

Use this query-parameter to get the summary output of nslimitidentifier resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/nslimitidentifier? **pagesize=#no;pageno=#no**

Use this query-parameter to get the nslimitidentifier resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nslimitidentifier": [ {

"limitidentifier":<String_value>,

"ngname":<String_value>,

"threshold":<Integer_value>,

"timeslice":<Integer_value>,

"mode":<String_value>,

"limittype":<String_value>,

"selectorname":<String_value>,

"hits":<Integer_value>,

"drop":<Integer_value>,

"rule":<String[]_value>,

"time":<Integer_value>,
```

```
"total":<Integer_value>,

"maxbandwidth":<Integer_value>,

"trapsintimeslice":<Integer_value>,

"trapscomputedintimeslice":<Integer_value>,

"computedtraptimeslice":<Integer_value>,

"alertsintimeslice":<Integer_value>,

"alertscomputedintimeslice":<Integer_value>,

"computedalerttimeslice":<Integer_value>,

"timealign":<String_value>,

"referencecount":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/nslimitidentifier/ limitidentifier_value<String>
Query-parameters: attrs http:// <netscaler-ip-address> /nitro/v1/config/nslimitidentifier/ limitidentifier_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/nslimitidentifier/ limitidentifier_value<String> ? **view=summary**

Use this query-parameter to get the summary output of nslimitidentifier resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "nslimitidentifier": [ {

"limitidentifier":<String_value>,

"ngname":<String_value>,

"threshold":<Integer_value>,

"timeslice":<Integer_value>,

"mode":<String_value>,

"limittype":<String_value>,

"selectorname":<String_value>,

"hits":<Integer_value>,

"drop":<Integer_value>,

"rule":<String[]_value>,

"time":<Integer_value>,

"total":<Integer_value>,

"maxbandwidth":<Integer_value>,
```

```
"trapsintimeslice":<Integer_value>,

"trapscomputedintimeslice":<Integer_value>,

"computedtraptimeslice":<Integer_value>,

"alertsintimeslice":<Integer_value>,

"alertscomputedintimeslice":<Integer_value>,

"computedalerttimeslice":<Integer_value>,

"timealign":<String_value>,

"referencecount":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/nslimitidentifier? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nslimitidentifier": [ { "__count": "#no"} ] }
```

nslimitidentifier_binding

Binding object which returns the resources bound to nslimitidentifier.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
limitidentifier	<String>	Read-write	Name of the rate limit identifier about which to display information. If a name is not provided, information about all rate limit identifiers is shown.
nslimitidentifier_nslimitsessions_binding	<nslimitidentifier_nslimitsessions_binding[]>	Read-only	nslimitsessions that can be bound to nslimitidentifier.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/nslimitidentifier_binding/limitidentifier_value<String>

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nslimitidentifier_binding": [ {

"limitidentifier":<String_value>,

"nslimitidentifier_nslimitsessions_binding":<nslimitidentifier_nslimitsess
ions_binding[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/nslimitidentifier_binding

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters:

bulkbindings

http:// <netscaler-ip-address> /nitro/v1/config/nslimitidentifier_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nslimitidentifier_binding": [ {

"limitidentifier":<String_value>,

"nslimitidentifier_nslimitsessions_binding":<nslimitidentifier_nslimitsessions_binding[]_value>

}]}
```

nslimitidentifier_nslimitsessions_binding

Binding object showing the nslimitsessions that can be bound to nslimitidentifier.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
limitidentifier	<String>	Read-write	Name of the rate limit identifier about which to display information. If a name is not provided, information about all rate limit identifiers is shown.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/nslimitidentifier_nslimitsessions_binding/limitidentifier_value<String>

Query-parameters:

filter

http:// <netscaler-ip-address> /nitro/v1/config/nslimitidentifier_nslimitsessions_binding/limitidentifier_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of nslimitidentifier_nslimitsessions_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination

http:// <netscaler-ip-address> /nitro/v1/config/nslimitidentifier_nslimitsessions_binding/ limitidentifier_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the nslimitidentifier_nslimitsessions_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "nslimitidentifier_nslimitsessions_binding": [ {

"limitidentifier":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/nslimitidentifier_nslimitsessions_binding

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters:

bulkbindings

http:// <netscaler-ip-address> /nitro/v1/config/nslimitidentifier_nslimitsessions_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "nslimitidentifier_nslimitsessions_binding": [ {

"limitidentifier":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/nslimitidentifier_nslimitsessions_binding/ limitidentifier_value<String> ? **count=yes**

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"nslimitidentifier_nslimitsessions_binding": [ { "__count": "#no"} ] }
```

nslimitselector

Configuration for limit selector resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
selectorname	<String>	Read-write	.
rule	<String[]>	Read-write	. Minimum length = 1
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE

- UNSET
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/nslimitselector **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nslimitselector":{

<b>"selectorname":<String_value>,

</b><b>"rule":<String[]_value>

</b>}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/nslimitselector/ selectorname_value<String>
HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/nslimitselector **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nslimitselector":{

<b>"selectorname":<String_value>,

</b>"rule":<String[]_value>
```

```
}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/nslimitselector? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nslimitselector":{

<b>"selectorname":<String_value>,

</b>"rule":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/nslimitselector **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/nslimitselector? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/nslimitselector? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of nslimitselector resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/nslimitselector? **view=summary**

Use this query-parameter to get the summary output of nslimitselector resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/nslimitselector? **pagesize=#no;pageno=#no**

Use this query-parameter to get the nslimitselector resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nslimitselector": [ {

"selectorname":<String_value>,

"rule":<String[]_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/nslimitselector/ selectorname_value<String>
Query-parameters: attrs http:// <netscaler-ip-address> /nitro/v1/config/nslimitselector/ selectorname_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/nslimitselector/ selectorname_value<String> ? **view=summary**

Use this query-parameter to get the summary output of nslimitselector resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "nslimitselector": [ {

"selectorname":<String_value>,

"rule":<String[]_value>,

"_nextgenapiresource":<String_value>

}]}
```

```
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/nslimitselector? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nslimitselector": [ { "__count": "#no"} ] }
```

nslimitsessions

Configuration for limit sessions resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
limitidentifier	<String>	Read-write	Name of the rate limit identifier for which to display the sessions. Minimum length = 1
detail	<Boolean>	Read-write	Show the individual hash values.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
timeout	<Integer>	Read-only	The time remaining on the session before a flush can be attempted. If active transactions are present the session will not be flushed.
hits	<Integer>	Read-only	The number of times this entry was hit.
drop	<Integer>	Read-only	The number of times action was taken.
number	<Integer[]>	Read-only	The hash of the matched selectlets.
name	<String>	Read-only	The string formed by gathering selectlet values.
unit	<Integer>	Read-only	Total computed hash of the matched selectlets.
flags	<Integer>	Read-only	Used internally to identify ip addresses.
referencecount	<Integer>	Read-only	Total number of transactions pointing to this entry. Its the sum total of the connection and bandwidth references.
maxbandwidth	<Integer>	Read-only	The current bandwidth.
selectoripv61	<String>	Read-only	First IPV6 address gathered.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
selectoripv62	<String>	Read-only	Second IPV6 address gathered.
flag	<Integer>	Read-only	Used internally to identify ipv6 addresses.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET (ALL)
- COUNT
- CLEAR

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

CLEAR

URL: http:// <netscaler-ip-address> /nitro/v1/config/nslimitsessions? **action=clear HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nslimitsessions":{

<b>"limitidentifier":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/nslimitsessions **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/nslimitsessions? **args= limitidentifier:<String_value>, detail: <Boolean_value>**

Use this query-parameter to get nslimitsessions resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/config/nslimitsessions? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/nslimitsessions? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of nslimitsessions resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/nslimitsessions? **view=summary**

Use this query-parameter to get the summary output of nslimitsessions resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/nslimitsessions? **pagesize=#no;pageno=#no**

Use this query-parameter to get the nslimitsessions resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nslimitsessions": [ {

<b>limitidentifier:<String_value>,</
b>detail:<Boolean_value>"timeout":<Integer_value>,

"hits":<Integer_value>,

"drop":<Integer_value>,

"number":<Integer[]_value>,
```

```
"name":<String_value>,

"unit":<Integer_value>,

"flags":<Integer_value>,

"referencecount":<Integer_value>,

"maxbandwidth":<Integer_value>,

"selectoripv61":<String_value>,

"selectoripv62":<String_value>,

"flag":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/nslimitsessions? **args= limitidentifier:<String_value>, detail: <Boolean_value> ;count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nslimitsessions": [ { "__count": "#no"} ] }
```

nsmemrecovery

Configuration for memory recovery operations resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
percentage	<Integer>	Read-write	Percentage of memory to be recovered from freepools. Default value: 10 Minimum value = 5 Maximum value = 90

Operations

(click to see Properties)

- START

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.
- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of

creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

START

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsmemrecovery? **action=start HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nsmemrecovery":{

"percentage":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

nsmgmtparam

Configuration for Management related configuration resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
mgmthttpport	<Integer>	Read-write	This allow the configuration of management HTTP port. Default value: 80 Minimum value = 1 Maximum value = 65534
mgmthttpsport	<Integer>	Read-write	This allows the configuration of management HTTPS port. Default value: 443 Minimum value = 1 Maximum value = 65534
httpdmaxclients	<Integer>	Read-write	This enables setting the HTTPD Max Clients value in the httpd.conf file. You can configure either Max Clients or Max Request Workers. The allowable range is from a minimum of 1 to a maximum of 255. Default value: 0 Minimum value = 0

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum value = 255
httpdmaxreqworkers	<Integer>	Read-write	This enables setting the HTTPD Max Request Workers value in the httpd.conf file. You can configure either Max Clients or Max Request Workers. The allowable range is from a minimum of 1 to a maximum of 255. Default value: 0 Minimum value = 0 Maximum value = 255
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- UPDATE
- UNSET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsmgmtparam **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nsmgmtparam":{

"mgmthttpport":<Integer_value>,

"mgmthttpsport":<Integer_value>,

"httpdmaxclients":<Integer_value>,

"httpdmaxreqworkers":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsmgmtparam? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nsmgmtparam":{

"mgmthttpport":true,

"mgmthttpsport":true,

"httpdmaxclients":true,

"httpdmaxreqworkers":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsmgmtparam **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nsmgmtparam": [ {

"mgmthttpport":<Integer_value>,

"mgmthttpsport":<Integer_value>,

"httpdmaxclients":<Integer_value>,

"httpdmaxreqworkers":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

nsmigration

Configuration for Migration operation resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
dumpsession	<String>	Read-write	Displays the current active migrated session details, if DUMPSESSION option is YES.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: NO Possible values = YES, NO
migrationstatus	<String>	Read-only	ISSU Migration Status. Possible values = Migration is not yet started, Migration is in progress and Failover is not yet done, Migration is in progress and Failover is completed, Rollback is initiated and Failover is not yet done, Rollback is initiated and Failover is completed, Migration is completed
migrationstarttime	<String>	Read-only	Timestamp for start migration. Minimum length = 1
migrationendtime	<String>	Read-only	Timestamp for migration complete. Minimum length = 1
migrationrollbackstarttime	<String>	Read-only	Timestamp for start migration rollback. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
srcip	<String>	Read-only	IP address to match against the source IP address of an incoming IPv4 packet.
srcport	<Integer>	Read-only	Port number to match against the source port number of an incoming IPv4 packet.
destip	<String>	Read-only	IP address to match against the destination IP address of an incoming IPv4 packet.
destport	<Integer>	Read-only	Port number to match against the destination port number of an incoming IPv4 packet.
timeout	<Integer>	Read-only	Time for which the connection is idle.
migdfdsessionsallocated	<Integer>	Read-only	Number of migration sessions allocated.
migdfdsessionsactive	<Integer>	Read-only	Number of migration sessions active.
migl4sessionsallocated	<Integer>	Read-only	Number of migration sessions allocated.
migl4sessionsactive	<Integer>	Read-only	Number of migration sessions active.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
migdfdsessionsallocatedrollback	<Integer>	Read-only	Number of migration sessions allocated.
migdfdsessionsactiverollback	<Integer>	Read-only	Number of migration sessions active.
migl4sessionsallocatedrollback	<Integer>	Read-only	Number of migration sessions allocated.
migl4sessionsactiverollback	<Integer>	Read-only	Number of migration sessions active.
mighastateflag	<Integer>	Read-only	Current master state in HA.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- START
- STOP
- COMPLETE
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

START

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsmigration? **action=start HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nsmigration":{

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

STOP

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsmigration? **action=stop HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nsmigration":{

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

COMPLETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsmigration? **action=complete HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nsmigration":{

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsmigration **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/nsmigration? **args=dumpsession: <String_value>**

Use this query-parameter to get nsmigration resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/config/nsmigration? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/nsmigration? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of nsmigration resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/nsmigration? **view=summary**

Use this query-parameter to get the summary output of nsmigration resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/nsmigration? **pagesize=#no;pageno=#no**

Use this query-parameter to get the nsmigration resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nsmigration": [ {

dumpsession:<String_value>"migrationstatus":<String_value>,

"migrationstarttime":<String_value>,

"migrationendtime":<String_value>,

"migrationrollbackstarttime":<String_value>,

"dumpsession":<String_value>,

"srcip":<String_value>,

"srcport":<Integer_value>,

"destip":<String_value>,

"destport":<Integer_value>,

"timeout":<Integer_value>,

"migdfdsessionsallocated":<Integer_value>,

"migdfdsessionsactive":<Integer_value>,

"migl4sessionsallocated":<Integer_value>,

"migl4sessionsactive":<Integer_value>,

"migdfdsessionsallocatedrollback":<Integer_value>,

"migdfdsessionsactiverollback":<Integer_value>,

"migl4sessionsallocatedrollback":<Integer_value>,

"migl4sessionsactiverollback":<Integer_value>,

"mighastateflag":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

```
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsmigration? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nsmigration": [ { "__count": "#no"} ] }
```

nsmode

Configuration for ns mode resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
mode	<String[]>	Read-write	Mode to be enabled. Multiple modes can be specified by providing a blank space between each mode. Possible values = FR, FastRamp, L2, L2mode, L3,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			L3mode, USIP, UseSourceIP, CKA, ClientKeepAlive, TCPB, TCPBuffering, MBF, MACbasedforwarding, Edge, USNIP, SRADV, DRADV, IRADV, SRADV6, DRADV6, PMTUD, RISE_APBR, RISE_RHI, BridgeBPDUs, SINGLE_IP, ULFD
fr	<Boolean>	Read-only	Fast Ramp.
l2	<Boolean>	Read-only	Layer 2 mode.
usip	<Boolean>	Read-only	Use Source IP.
cka	<Boolean>	Read-only	Client Keep-alive.
tcpb	<Boolean>	Read-only	TCP Buffering.
mbf	<Boolean>	Read-only	MAC-based forwarding.
edge	<Boolean>	Read-only	Edge configuration.
usnip	<Boolean>	Read-only	Use Subnet IP.
l3	<Boolean>	Read-only	Layer 3 mode (ip forwarding).
pmtud	<Boolean>	Read-only	Path MTU Discovery.
mediaclassification	<Boolean>	Read-only	mediaclassification.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
sradv	<Boolean>	Read-only	Static Route Advertisement.
dradv	<Boolean>	Read-only	Direct Route Advertisement.
iradv	<Boolean>	Read-only	Intranet Route Advertisement.
sradv6	<Boolean>	Read-only	Ipv6 Static Route Advertisement.
dradv6	<Boolean>	Read-only	Ipv6 Direct Route Advertisement.
bridgebpdus	<Boolean>	Read-only	BPDU Bridging Mode.
single_ip	<Boolean>	Read-only	Single IP mode.
ulfd	<Boolean>	Read-only	Unified Logging Framework Mode for adding/removing ULF services.
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- ENABLE
- DISABLE
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ENABLE

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsmode? **action=enable HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nsmode":{

"mode":<String[]_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DISABLE

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsmode? **action=disable HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nsmode":{

"mode":<String[]_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsmode **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nsmode": [ {

"mode":<String[]_value>,

"fr":<Boolean_value>,

"l2":<Boolean_value>,

"usip":<Boolean_value>,

"cka":<Boolean_value>,

"tcpb":<Boolean_value>,

"mbf":<Boolean_value>,

"edge":<Boolean_value>,

"usnip":<Boolean_value>,

"l3":<Boolean_value>,

"pmtud":<Boolean_value>,

"mediaclassification":<Boolean_value>,

"sradv":<Boolean_value>,

"dradv":<Boolean_value>,

"iradv":<Boolean_value>,

"sradv6":<Boolean_value>,

"dradv6":<Boolean_value>,

"bridgebpdus":<Boolean_value>,

"single_ip":<Boolean_value>,

"ulfd":<Boolean_value>,
```

```
"_nextgenapiresource":<String_value>

}]}
```

nsnextgenapi

Configuration for 0 resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
state	<String>	Read-write	NextGen API state. Possible values = ENABLED, DISABLED
_nextgenapiresource	<String>	Read-write	.

Operations

(click to see Properties)

- ENABLE
- DISABLE
- CLEAR
- RESET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ENABLE

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsnextgenapi? **action=enable HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nsnextgenapi":{

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DISABLE

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsnextgenapi? **action=disable HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nsnextgenapi":{

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

CLEAR

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsnextgenapi? **action=clear HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nsnextgenapi":{

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

RESET

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsnextgenapi? **action=reset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nsnextgenapi":{

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsnextgenapi **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nsnextgenapi": [ {

"state":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

nsparam

Configuration for Citrix ADC parameters resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
httpport	<Integer[]>	Read-write	HTTP ports on the web server. This allows the system to perform connection off-load for any client request that has a destination port matching one of these configured ports. Minimum value = 1 Maximum value = 65535
maxconn	<Integer>	Read-write	Maximum number of connections that will be made from the appliance to the web server(s) attached to it. The value entered here is applied globally to all attached servers.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: 0 Minimum value = 0 Maximum value = 4294967294
maxreq	<Integer>	Read-write	Maximum number of requests that the system can pass on a particular connection between the appliance and a server attached to it. Setting this value to 0 allows an unlimited number of requests to be passed. This value is overridden by the maximum number of requests configured on the individual service. Minimum value = 0 Maximum value = 65535
cip	<String>	Read-write	Enable or disable the insertion of the actual client IP address into the HTTP header request passed from the client to one, some, or all servers attached to the system. The passed address can then be accessed through a

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			minor modification to the server. * If the CIP header is specified, it will be used as the client IP header. * If the CIP header is not specified, the value that has been set will be used as the client IP header. Possible values = ENABLED, DISABLED
cipheader	<String>	Read-write	Text that will be used as the client IP address header. Minimum length = 1
cookieversion	<String>	Read-write	Version of the cookie inserted by the system. Possible values = 0, 1
securecookie	<String>	Read-write	Enable or disable secure flag for persistence cookie. Default value: ENABLED Possible values = ENABLED, DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
pmtumin	<Integer>	Read-write	Minimum path MTU value that Citrix ADC will process in the ICMP fragmentation needed message. If the ICMP message contains a value less than this value, then this value is used instead. Default value: 576 Minimum value = 168 Maximum value = 1500
pmtutimeout	<Integer>	Read-write	Interval, in minutes, for flushing the PMTU entries. Default value: 10 Minimum value = 1 Maximum value = 1440
ftpportrange	<String>	Read-write	Minimum and maximum port (port range) that FTP services are allowed to use. Minimum length = 1024 Maximum length = 64000

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
crportrange	<String>	Read-write	Port range for cache redirection services. Minimum length = 1 Maximum length = 65535
timezone	<String>	Read-write	Time zone for the Citrix ADC. Name of the time zone should be specified as argument. Default value: CoordinatedUniversalTime Minimum length = 1 Maximum length = 63
grantquotamaxclient	<Integer>	Read-write	Percentage of shared pool value granted to PE once PE exhausts the local exclusive quota. Where shared pool is the remaining maxclient quota after distribution of exclusive quota to PEs. Example: In a 2 PE NetScaler system if configured maxclient is 100 and exclusive quota is 80 percent then each PE will get 40

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			as local exclusive quota and 20 will be in shared pool. If configured grantQuota is 20 percent, then after exhausting its local exclusive quota PE borrows from shared pool in chunks of 4 i.e. 20 percent of 20. Default value: 10 Minimum value = 0 Maximum value = 100
exclusivequotamaxclient	<Integer>	Read-write	Percentage of maxClient threshold to be divided equally among PEs. Default value: 80 Minimum value = 0 Maximum value = 100
grantquotaspillover	<Integer>	Read-write	Percentage of shared pool value granted to PE once PE exhausts the local exclusive quota. Where shared pool is the remaining spillover quota after distribution of

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			exclusive quota to PEs. Example: In a 2 PE NetScaler system if configured spillover is 100 and exclusive quota is 80 percent then each PE will get 40 as local exclusive quota and 20 will be in shared pool. If configured grantQuota is 20 percent, then after exhausting its local exclusive quota PE borrows from shared pool in chunks of 4 i.e. 20 percent of 20. Default value: 10 Minimum value = 0 Maximum value = 100
exclusivequotaspillover	<Integer>	Read-write	Percentage of spillover threshold to be divided equally among PEs. Default value: 80 Minimum value = 0 Maximum value = 100

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
useproxyport	<String>	Read-write	Enable/Disable use_proxy_port setting. Default value: ENABLED Possible values = ENABLED, DISABLED
internaluserlogin	<String>	Read-write	Enables/disables the internal user from logging in to the appliance. Before disabling internal user login, you must have key-based authentication set up on the appliance. The file name for the key pair must be "ns_comm_key". Default value: ENABLED Possible values = ENABLED, DISABLED
aftpallowrandomsourceport	<String>	Read-write	Allow the FTP server to come from a random source port for active FTP data connections. Default value: DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ENABLED, DISABLED
icaports	<Integer[]>	Read-write	The ICA ports on the Web server. This allows the system to perform connection off-load for any client request that has a destination port matching one of these configured ports. Minimum value = 1
tcpcip	<String>	Read-write	Enable or disable the insertion of the client TCP/IP header in TCP payload passed from the client to one, some, or all servers attached to the system. The passed address can then be accessed through a minor modification to the server. Default value: DISABLED Possible values = ENABLED, DISABLED
servicepathingressvlan	<Integer>	Read-write	VLAN on which the subscriber traffic arrives on the appliance.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum value = 1
secureicaports	<Integer[]>	Read-write	The Secure ICA ports on the Web server. This allows the system to perform connection off-load for any client request that has a destination port matching one of these configured ports. Minimum value = 1
mgmthttpport	<Integer>	Read-write	This allow the configuration of management HTTP port. Default value: 80 Minimum value = 1 Maximum value = 65534
mgmthttpsport	<Integer>	Read-write	This allows the configuration of management HTTPS port. Default value: 443 Minimum value = 1 Maximum value = 65534
proxyprotocol	<String>	Read-write	Disable/Enable v1 or v2 proxy protocol

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			header for client info insertion. Default value: DISABLED Possible values = ENABLED, DISABLED
advancedanalyticsstats	<String>	Read-write	Disable/Enable advanace analytics stats. Default value: DISABLED Possible values = ENABLED, DISABLED
ipttl	<Integer>	Read-write	Set the IP Time to Live (TTL) and Hop Limit value for all outgoing packets from Citrix ADC. Default value: 255 Minimum value = 1 Maximum value = 255
autoscaleoption	<Integer>	Read-only	64 bits are provided for communication between ADM and ADC in cloud deployments. Currently LSB 3 bits are used.0x01=>AWS,0x

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			02=>Azure,0x04=>GCP. Default value: 0
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- UPDATE
- UNSET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsparam **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nsparam":{

"httpport":<Integer[]_value>,

"maxconn":<Integer_value>,

"maxreq":<Integer_value>,

"cip":<String_value>,

"cipheader":<String_value>,

"cookieversion":<String_value>,

"securecookie":<String_value>,

"pmtumin":<Integer_value>,

"pmtutimeout":<Integer_value>,

"ftpportrange":<String_value>,

"crportrange":<String_value>,

"timezone":<String_value>,

"grantquotamaxclient":<Integer_value>,

"exclusivequotamaxclient":<Integer_value>,

"grantquotaspillover":<Integer_value>,

"exclusivequotaspillover":<Integer_value>,
```

```
"useproxyport":<String_value>,

"internaluserlogin":<String_value>,

"aftpallowrandomsourceport":<String_value>,

"icaports":<Integer[]_value>,

"tcpcip":<String_value>,

"servicepathingressvlan":<Integer_value>,

"secureicaports":<Integer[]_value>,

"mgmthttpport":<Integer_value>,

"mgmthttpsport":<Integer_value>,

"proxyprotocol":<String_value>,

"advancedanalyticsstats":<String_value>,

"ipttl":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsparam? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nsparam":{

"ftpportrange":true,

"crportrange":true,

"aftpallowrandomsourceport":true,

"httpport":true,

"maxconn":true,

"maxreq":true,

"cip":true,

"cipheader":true,

"cookieversion":true,

"securecookie":true,

"pmtumin":true,

"pmtutimeout":true,

"timezone":true,

"grantquotamaxclient":true,

"exclusivequotamaxclient":true,

"grantquotaspillover":true,

"exclusivequotaspillover":true,

"useproxyport":true,

"internaluserlogin":true,

"icaports":true,

"tcpcip":true,
```

```
"servicepathingressvlan":true,

"secureicaports":true,

"mgmthttpport":true,

"mgmthttpsport":true,

"proxyprotocol":true,

"advancedanalyticsstats":true,

"ipttl":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsparam **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nsparam": [ {

"httpport":<Integer[]_value>,

"maxconn":<Integer_value>,

"maxreq":<Integer_value>,

"cip":<String_value>,

"cipheader":<String_value>,

"cookieversion":<String_value>,

"securecookie":<String_value>,

"pmtumin":<Integer_value>,

"pmtutimeout":<Integer_value>,

"ftpportrange":<String_value>,

"crportrange":<String_value>,

"timezone":<String_value>,

"grantquotamaxclient":<Integer_value>,

"exclusivequotamaxclient":<Integer_value>,

"grantquotaspillover":<Integer_value>,

"exclusivequotaspillover":<Integer_value>,

"useproxyport":<String_value>,

"internaluserlogin":<String_value>,

"aftpallowrandomsourceport":<String_value>,

"icaports":<Integer[]_value>,

"tcpcip":<String_value>,
```

```
"servicepathingressvlan":<Integer_value>,

"secureicaports":<Integer[]_value>,

"mgmthttpport":<Integer_value>,

"mgmthttpsport":<Integer_value>,

"proxyprotocol":<String_value>,

"advancedanalyticsstats":<String_value>,

"autoscaleoption":<Integer_value>,

"ipttl":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

nspartition

Configuration for admin partition resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
partitionname	<String>	Read-write	Name of the Partition. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			hyphen (-) characters. Minimum length = 1
maxbandwidth	<Integer>	Read-write	Maximum bandwidth, in Kbps, that the partition can consume. A zero value indicates the bandwidth is unrestricted on the partition and it can consume up to the system limits. Default value: 10240
minbandwidth	<Integer>	Read-write	Minimum bandwidth, in Kbps, that the partition can consume. A zero value indicates the bandwidth is unrestricted on the partition and it can consume up to the system limits. Default value: 10240
maxconn	<Integer>	Read-write	Maximum number of concurrent connections that can be open in the partition. A zero value indicates no limit on number of open connections. Default value: 1024

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
maxmemlimit	<Integer>	Read-write	Maximum memory, in megabytes, allocated to the partition. A zero value indicates the memory is unlimited on the partition and it can consume up to the system limits. Default value: 10 Minimum value = 0 Maximum value = 1048576
partitionmac	<String>	Read-write	Special MAC address for the partition which is used for communication over shared vlans in this partition. If not specified, the MAC address is auto-generated.
force	<Boolean>	Read-write	Switches to new admin partition without prompt for saving configuration. Configuration will not be saved.
save	<Boolean>	Read-write	Switches to new admin partition without prompt for saving configuration. Configuration will be saved.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
partitionid	<Integer>	Read-only	Partition Id. Minimum value = 1 Maximum value = 511
partitiontype	<String>	Read-only	Type of the Partition. Possible values = Default Partition, Current Partition
pmacinternal	<Boolean>	Read-only	Partition MAC is generated internally.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- SWITCH
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/nspartition **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nspartition":{

<b>"partitionname":<String_value>,

</b>"maxbandwidth":<Integer_value>,

"minbandwidth":<Integer_value>,

"maxconn":<Integer_value>,

"maxmemlimit":<Integer_value>,

"partitionmac":<String_value>
```

```
}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/nspartition/ partitionname_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/nspartition **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nspartition":{

<b>"partitionname":<String_value>,

</b>"maxbandwidth":<Integer_value>,

"minbandwidth":<Integer_value>,

"maxconn":<Integer_value>,

"maxmemlimit":<Integer_value>,
```

```
"partitionmac":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/nspartition? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nspartition":{

<b>"partitionname":<String_value>,

</b>"maxbandwidth":true,

"minbandwidth":true,

"maxconn":true,

"maxmemlimit":true,

"partitionmac":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

SWITCH

URL: http:// <netscaler-ip-address> /nitro/v1/config/nspartition? **action=Switch HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nspartition":{

<b>"partitionname":<String_value>,

</b>"force":<Boolean_value>,

"save":<Boolean_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/nspartition **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/nspartition? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/nspartition? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of nspartition resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/nspartition? **view=summary**

Use this query-parameter to get the summary output of nspartition resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/nspartition? **pagesize=#no;pageno=#no**

Use this query-parameter to get the nspartition resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nspartition": [ {

"partitionname":<String_value>,

"partitionid":<Integer_value>,

"partitiontype":<String_value>,

"maxbandwidth":<Integer_value>,

"minbandwidth":<Integer_value>,

"maxconn":<Integer_value>,

"maxmemlimit":<Integer_value>,
```

```
"partitionmac":<String_value>,

"pmacinternal":<Boolean_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/nspartition/ partitionname_value<String>
Query-parameters: attrs http:// <netscaler-ip-address> /nitro/v1/config/nspartition/ partitionname_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/nspartition/ partitionname_value<String> ? **view=summary**

Use this query-parameter to get the summary output of nspartition resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "nspartition": [ {

"partitionname":<String_value>,

"partitionid":<Integer_value>,

"partitiontype":<String_value>,

"maxbandwidth":<Integer_value>,

"minbandwidth":<Integer_value>,

"maxconn":<Integer_value>,

"maxmemlimit":<Integer_value>,

"partitionmac":<String_value>,

"pmacinternal":<Boolean_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/nspartition? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nspartition": [ { "__count": "#no"} ] }
```

nspartition_binding

Binding object which returns the resources bound to nspartition.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
partitionname	<String>	Read-write	Name of partition for which to display parameters. Minimum length = 1
nspartition_vlan_binding	<nspartition_vlan_binding[]>	Read-only	vlan that can be bound to nspartition.
nspartition_bridgegroup_binding	<nspartition_bridgegroup_binding[]>	Read-only	bridgegroup that can be bound to nspartition.
nspartition_vxlan_binding	<nspartition_vxlan_binding[]>	Read-only	vxlan that can be bound to nspartition.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/nspartition_binding/ partitionname_value<String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nspartition_binding": [ {

"partitionname":<String_value>,
```

```
"nspartition_bridgegroup_binding":<nspartition_bridgegroup_binding[]_value
>,

"nspartition_vlan_binding":<nspartition_vlan_binding[]_value>,

"nspartition_vxlan_binding":<nspartition_vxlan_binding[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/nspartition_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/nspartition_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nspartition_binding": [ {

"partitionname":<String_value>,

"nspartition_bridgegroup_binding":<nspartition_bridgegroup_binding[]_value
>,
```

```
"nspartition_vlan_binding":<nspartition_vlan_binding[]_value>,

"nspartition_vxlan_binding":<nspartition_vxlan_binding[]_value>

}]}
```

nspartition_bridgegroup_binding

Binding object showing the bridgegroup that can be bound to nspartition.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
partitionname	<String>	Read-write	Name of the Partition. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Minimum length = 1
bridgegroup	<Integer>	Read-write	Identifier of the bridge group that is assigned to this partition. Minimum value = 1 Maximum value = 1000

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/nspartition_bridgegroup_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"nspartition_bridgegroup_binding":{

<b>"partitionname":<String_value>,

</b>"bridgegroup":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/nspartition_bridgegroup_binding/ partitionname_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/ config/nspartition_bridgegroup_binding/ partitionname_value<String> ? **args=bridgegroup: <Integer_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/nspartition_bridgegroup_binding/ partitionname_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/ config/nspartition_bridgegroup_binding/ partitionname_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of nspartition_bridgegroup_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/nspartition_bridgegroup_binding/ partitionname_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the nspartition_bridgegroup_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "nspartition_bridgegroup_binding": [ {

"partitionname":<String_value>,

"bridgegroup":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/nspartition_bridgegroup_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/nspartition_bridgegroup_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "nspartition_bridgegroup_binding": [ {

"partitionname":<String_value>,

"bridgegroup":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/nspartition_bridgegroup_binding/partitionname_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"nspartition_bridgegroup_binding": [ { "__count": "#no"} ] }
```

nspartition_vlan_binding

Binding object showing the vlan that can be bound to nspartition.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
vlan	<Integer>	Read-write	Identifier of the vlan that is assigned to this partition. Minimum value = 1 Maximum value = 4094
partitionname	<String>	Read-write	Name of the Partition. Must begin with an ASCII alphanumeric or underscore (_) character, and must

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Minimum length = 1
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/nspartition_vlan_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"nspartition_vlan_binding":{

<b>"partitionname":<String_value>,

</b>"vlan":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/nspartition_vlan_binding/ partitionname_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/ config/nspartition_vlan_binding/ partitionname_value<String> ? **args=vlan: <Integer_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/nspartition_vlan_binding/ partitionname_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/ config/nspartition_vlan_binding/ partitionname_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of nspartition_vlan_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/nspartition_vlan_binding/ partitionname_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the nspartition_vlan_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "nspartition_vlan_binding": [ {

"vlan":<Integer_value>,

"partitionname":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/nspartition_vlan_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/nspartition_vlan_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "nspartition_vlan_binding": [ {

"vlan":<Integer_value>,

"partitionname":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/nspartition_vlan_binding/ partitionname_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"nspartition_vlan_binding": [ { "__count": "#no"} ] }
```

nspartition_vxlan_binding

Binding object showing the vxlan that can be bound to nspartition.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
vxlan	<Integer>	Read-write	Identifier of the vxlan that is assigned to this partition. Minimum value = 1 Maximum value = 16777215

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
partitionname	<String>	Read-write	Name of the Partition. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Minimum length = 1
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/nspartition_vxlan_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"nspartition_vxlan_binding":{

<b>"partitionname":<String_value>,

</b>"vxlan":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/nspartition_vxlan_binding/ partitionname_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/ config/nspartition_vxlan_binding/ partitionname_value<String> ? **args=vxlan: <Integer_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/nspartition_vxlan_binding/ partitionname_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/ config/nspartition_vxlan_binding/ partitionname_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of nspartition_vxlan_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/nspartition_vxlan_binding/ partitionname_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the nspartition_vxlan_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "nspartition_vxlan_binding": [ {

"vxlan":<Integer_value>,

"partitionname":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/nspartition_vxlan_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/nspartition_vxlan_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "nspartition_vxlan_binding": [ {

"vxlan":<Integer_value>,
```

```
"partitionname":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/nspartition_vxlan_binding/ partitionname_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"nspartition_vxlan_binding": [ { "__count": "#no"} ] }
```

nspartitionmac

Configuration for partition MACs resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
partitionmac	<String>	Read-write	A configured virtual MAC address that can be used by a partition for

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			communication over shared VLANs.
partitionname	<String>	Read-write	Name of the partition to which the MAC has been assigned. Minimum length = 1
_nextgenapiresource	<String>	Read-write	.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/nspartitionmac **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/nspartitionmac? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/nspartitionmac? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of nspartitionmac resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/nspartitionmac? **view=summary**

Use this query-parameter to get the summary output of nspartitionmac resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/nspartitionmac? **pagesize=#no;pageno=#no**

Use this query-parameter to get the nspartitionmac resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nspartitionmac": [ {

"partitionmac":<String_value>,

"partitionname":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/nspartitionmac? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nspartitionmac": [ { "__count": "#no"} ] }
```

nspbr

Configuration for Policy Based Routing(PBR) entry resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the PBR. Must begin with an ASCII alphabetic or underscore \(_\) character, and must contain only ASCII alphanumeric, underscore, hash \(#\), period \(.\), space, colon \(:\), at \(@\), equals \(=\), and hyphen \(-\) characters. Cannot be changed after the PBR is created. Minimum length = 1
action	<String>	Read-write	Action to perform on the outgoing IPv4 packets that match the PBR. Available settings function as follows: * ALLOW - The Citrix ADC sends the packet to the designated next-hop router. * DENY - The Citrix ADC applies the routing table for normal destination-based routing. Possible values = ALLOW, DENY

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
td	<Integer>	Read-write	Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0. Minimum value = 0 Maximum value = 4094
srcip	<Boolean>	Read-write	IP address or range of IP addresses to match against the source IP address of an outgoing IPv4 packet. In the command line interface, separate the range with a hyphen. For example: 10.102.29.30-10.102.29.189.
srcipop	<String>	Read-write	Either the equals (=) or does not equal (!=) logical operator. Possible values = =, !=, EQ, NEQ
srcipval	<String>	Read-write	IP address or range of IP addresses to match against the source IP address of an outgoing IPv4

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			packet. In the command line interface, separate the range with a hyphen. For example: 10.102.29.30-10.102.29.189.
srcipdataset	<String>	Read-write	Policy dataset which can have multiple IP ranges bound to it.
srcport	<Boolean>	Read-write	Port number or range of port numbers to match against the source port number of an outgoing IPv4 packet. In the command line interface, separate the range with a hyphen. For example: 40-90. Note: The destination port can be specified only for TCP and UDP protocols.
srcportop	<String>	Read-write	Either the equals (=) or does not equal (!=) logical operator. Possible values = =, !=, EQ, NEQ
srcportval	<String>	Read-write	Port number or range of port numbers to match

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			against the source port number of an outgoing IPv4 packet. In the command line interface, separate the range with a hyphen. For example: 40-90. Note: The destination port can be specified only for TCP and UDP protocols. Maximum length = 65535
srcportdataset	<String>	Read-write	Policy dataset which can have multiple port ranges bound to it.
destip	<Boolean>	Read-write	IP address or range of IP addresses to match against the destination IP address of an outgoing IPv4 packet. In the command line interface, separate the range with a hyphen. For example: 10.102.29.30-10.102.29.189.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
destipop	<String>	Read-write	Either the equals (=) or does not equal (!=) logical operator. Possible values = =, !=, EQ, NEQ
destipval	<String>	Read-write	IP address or range of IP addresses to match against the destination IP address of an outgoing IPv4 packet. In the command line interface, separate the range with a hyphen. For example: 10.102.29.30-10.102.29.189.
destipdataset	<String>	Read-write	Policy dataset which can have multiple IP ranges bound to it.
destport	<Boolean>	Read-write	Port number or range of port numbers to match against the destination port number of an outgoing IPv4 packet. In the command line interface, separate the range with a hyphen. For example: 40-90. Note: The destination port can

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			be specified only for TCP and UDP protocols.
destportop	<String>	Read-write	Either the equals (=) or does not equal (!=) logical operator. Possible values = =, !=, EQ, NEQ
destportval	<String>	Read-write	Port number or range of port numbers to match against the destination port number of an outgoing IPv4 packet. In the command line interface, separate the range with a hyphen. For example: 40-90. Note: The destination port can be specified only for TCP and UDP protocols. Maximum length = 65535
destportdataset	<String>	Read-write	Policy dataset which can have multiple port ranges bound to it.
nexthop	<Boolean>	Read-write	IP address of the next hop router or the name of the link

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			load balancing virtual server to which to send matching packets if action is set to ALLOW. If you specify a link load balancing (LLB) virtual server, which can provide a backup if a next hop link fails, first make sure that the next hops bound to the LLB virtual server are actually next hops that are directly connected to the Citrix ADC. Otherwise, the Citrix ADC throws an error when you attempt to create the PBR. The next hop can be null to represent null routes.
nexthopval	<String>	Read-write	The Next Hop IP address or gateway name.
iptunnel	<Boolean>	Read-write	The Tunnel name.
iptunnelname	<String>	Read-write	The iptunnel name where packets need to be forwarded upon.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
vxlanvlanmap	<String>	Read-write	The vlan to vxlan mapping to be applied for incoming packets over this pbr tunnel.
targettd	<Integer>	Read-write	Integer value that uniquely identifies the traffic domain to which you want to send packet to. Minimum value = 0 Maximum value = 4094
srcmac	<String>	Read-write	MAC address to match against the source MAC address of an outgoing IPv4 packet.
srcmacmask	<String>	Read-write	Used to define range of Source MAC address. It takes string of 0 and 1, 0s are for exact match and 1s for wildcard. For matching first 3 bytes of MAC address, srcMacMask value "000000111111". . Default value: "000000000000"
protocol	<String>	Read-write	Protocol, identified by protocol name, to match against the protocol of an

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			outgoing IPv4 packet. Possible values = ICMP, IGMP, TCP, EGP, IGP, ARGUS, UDP, RDP, RSVP, EIGRP, L2TP, ISIS, GGP, IPoverIP, ST, CBT, BBN-RCC-M, NVP-II, PUP, EMCON, XNET, CHAOS, MUX, DCN-MEAS, HMP, PRM, XNS-IDP, TRUNK-1, TRUNK-2, LEAF-1, LEAF-2, IRTP, ISO-TP4, NETBLT, MFE-NSP, MERIT-INP, SEP, 3PC, IDPR, XTP, DDP, IDPR-CMTP, TP++, IL, IPv6, SDRP, IPv6-Route, IPv6-Frag, IDRP, GRE, MHRP, BNA, ESP, AH, I-NLSP, SWIPE, NARP, MOBILE, TLSP, SKIP, ICMPV6, IPv6-NoNx, IPv6-Opts, Any-Host-Internal-Protocol, CFTP, Any-Local-Network, SAT-EXPAK,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			KRYPTOLAN, RVD, IPPC, Any-Distributed-File-System, TFTP, VISA, IPCV, CPNX, CPHB, WSN, PVP, BR-SAT-MO, SUN-ND, WB-MON, WB-EXPAK, ISO-IP, VMTP, SECURE-VM, VINES, TTP, NSFNET-IG, DGP, TCF, OSPFIGP, Sprite-RP, LARP, MTP, AX.25, IPIP, MICP, SCC-SP, ETHERIP, Any-Private-Encryption-Scheme, GMTP, IFMP, PNNI, PIM, ARIS, SCPS, QNX, A/N, IPComp, SNP, Compaq-Pe, IPX-in-IP, VRRP, PGM, Any-0-Hop-Protocol, ENCAP, DDX, IATP, STP, SRP, UTI, SMP, SM, PTP, FIRE, CRTP, CRUDP, SSCOPMCE, IPLT, SPS, PIPE, SCTP, FC, RSVP-E2E-IGNORE, Mobility-Header, UDPLite

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
protocolnumber	<Integer>	Read-write	Protocol, identified by protocol number, to match against the protocol of an outgoing IPv4 packet. Minimum value = 1 Maximum value = 255
vlan	<Integer>	Read-write	ID of the VLAN. The Citrix ADC compares the PBR only to the outgoing packets on the specified VLAN. If you do not specify any interface ID, the appliance compares the PBR to the outgoing packets on all VLANs. Minimum value = 1 Maximum value = 4094
vxlan	<Integer>	Read-write	ID of the VXLAN. The Citrix ADC compares the PBR only to the outgoing packets on the specified VXLAN. If you do not specify any interface ID, the appliance compares the PBR to the outgoing packets on all VXLANs.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum value = 1 Maximum value = 16777215
Interface	<String>	Read-write	ID of an interface. The Citrix ADC compares the PBR only to the outgoing packets on the specified interface. If you do not specify any value, the appliance compares the PBR to the outgoing packets on all interfaces.
priority	<Integer>	Read-write	Priority of the PBR, which determines the order in which it is evaluated relative to the other PBRs. If you do not specify priorities while creating PBRs, the PBRs are evaluated in the order in which they are created. Minimum value = 1 Maximum value = 81920
msr	<String>	Read-write	Monitor the route specified byte Next Hop parameter. This parameter is not applicable if you specify a link load balancing (LLB)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			virtual server name with the Next Hop parameter. Default value: DISABLED Possible values = ENABLED, DISABLED
monitor	<String>	Read-write	The name of the monitor.(Can be only of type ping or ARP). Minimum length = 1
state	<String>	Read-write	Enable or disable the PBR. After you apply the PBRs, the Citrix ADC compares outgoing packets to the enabled PBRs. Default value: ENABLED Possible values = ENABLED, DISABLED
ownergroup	<String>	Read-write	The owner node group in a Cluster for this pbr rule. If ownernode is not specified then the pbr rule is treated as Striped pbr rule. Default value: DEFAULT_NG Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
detail	<Boolean>	Read-write	To get a detailed view.
hits	<Integer>	Read-only	The hits of this PBR.
kernelstate	<String>	Read-only	The commit status of the PBR. Default value: NOTAPPLIED Possible values = APPLIED, NOTAPPLIED, RE-APPLY, SFAPPLIED, SFNOTAPPLIED, SFAPPLIED61, SFNOTAPPLIED61
curstate	<Integer>	Read-only	If this route is UP/DOWN.
totalprobes	<Integer>	Read-only	The total number of probes sent.
totalfailedprobes	<Integer>	Read-only	The total number of failed probes.
failedprobes	<Integer>	Read-only	Number of the current failed monitoring probes.
monstatcode	<Integer>	Read-only	The code indicating the monitor response.
monstatparam1	<Integer>	Read-only	First parameter for use with message code.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
monstatparam2	<Integer>	Read-only	Second parameter for use with message code.
monstatparam3	<Integer>	Read-only	Third parameter for use with message code.
data	<Boolean>	Read-only	Internal data of this route.
pbrchildcount	<Integer>	Read-only	Number of childs for this PBR, in case of dataset this will be number of ips bound to that dataset.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- ENABLE
- DISABLE
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/nspbr **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nspbr":{

<b>"name":<String_value>,

</b><b>"action":<String_value>,

</b>"td":<Integer_value>,
```

```
"srcip":<Boolean_value>,

"srcipop":<String_value>,

"srcipval":<String_value>,

"srcipdataset":<String_value>,

"srcport":<Boolean_value>,

"srcportop":<String_value>,

"srcportval":<String_value>,

"srcportdataset":<String_value>,

"destip":<Boolean_value>,

"destipop":<String_value>,

"destipval":<String_value>,

"destipdataset":<String_value>,

"destport":<Boolean_value>,

"destportop":<String_value>,

"destportval":<String_value>,

"destportdataset":<String_value>,

"nexthop":<Boolean_value>,

"nexthopval":<String_value>,

"iptunnel":<Boolean_value>,

"iptunnelname":<String_value>,

"vxlanvlanmap":<String_value>,

"targettd":<Integer_value>,
```

```
"srcmac":<String_value>,

"srcmacmask":<String_value>,

"protocol":<String_value>,

"protocolnumber":<Integer_value>,

"vlan":<Integer_value>,

"vxlan":<Integer_value>,

"Interface":<String_value>,

"priority":<Integer_value>,

"msr":<String_value>,

"monitor":<String_value>,

"state":<String_value>,

"ownergroup":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/nspbr/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/nspbr **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nspbr":{

<b>"name":<String_value>,

</b>"action":<String_value>,

"srcip":<Boolean_value>,

"srcipop":<String_value>,

"srcipval":<String_value>,

"srcport":<Boolean_value>,

"srcportop":<String_value>,

"srcportval":<String_value>,

"destip":<Boolean_value>,

"destipop":<String_value>,

"destipval":<String_value>,

"destport":<Boolean_value>,

"destportop":<String_value>,

"destportval":<String_value>,
```

```
"nexthop":<Boolean_value>,

"nexthopval":<String_value>,

"iptunnel":<Boolean_value>,

"iptunnelname":<String_value>,

"vxlanvlanmap":<String_value>,

"targettd":<Integer_value>,

"srcmac":<String_value>,

"srcmacmask":<String_value>,

"protocol":<String_value>,

"protocolnumber":<Integer_value>,

"vlan":<Integer_value>,

"vxlan":<Integer_value>,

"Interface":<String_value>,

"priority":<Integer_value>,

"msr":<String_value>,

"monitor":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/nspbr? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nspbr":{

<b>"name":<String_value>,

</b>"srcip":true,

"srcport":true,

"destip":true,

"destport":true,

"nexthop":true,

"iptunnel":true,

"vxlanvlanmap":true,

"targettd":true,

"srcmac":true,

"srcmacmask":true,

"protocol":true,

"vlan":true,

"vxlan":true,

"Interface":true,

"msr":true,

"monitor":true
```

```
}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

ENABLE

URL: http:// <netscaler-ip-address> /nitro/v1/config/nspbr? **action=enable HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nspbr":{

<b>"name":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DISABLE

URL: http:// <netscaler-ip-address> /nitro/v1/config/nspbr? **action=disable HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nspbr":{

<b>"name":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/nspbr **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/nspbr? **args=name: <String_value> ,detail: <Boolean_value>**

Use this query-parameter to get nspbr resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/config/nspbr? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/nspbr? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of nspbr resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/nspbr? **view=summary**

Use this query-parameter to get the summary output of nspbr resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/nspbr? **pagesize=#no;pageno=#no**

Use this query-parameter to get the nspbr resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nspbr": [ {

name:<String_value>,detail:<Boolean_value>"action":<String_value>,

"srcmac":<String_value>,

"srcmacmask":<String_value>,

"protocol":<String_value>,

"protocolnumber":<Integer_value>,

"srcportval":<String_value>,

"srcportdataset":<String_value>,

"srcportop":<String_value>,

"td":<Integer_value>,

"destportval":<String_value>,

"destportdataset":<String_value>,

"destportop":<String_value>,

"srcipval":<String_value>,

"srcipdataset":<String_value>,
```

```
"srcipop":<String_value>,

"destipval":<String_value>,

"destipop":<String_value>,

"destipdataset":<String_value>,

"vlan":<Integer_value>,

"vxlan":<Integer_value>,

"state":<String_value>,

"Interface":<String_value>,

"hits":<Integer_value>,

"priority":<Integer_value>,

"kernelstate":<String_value>,

"nexthopval":<String_value>,

"iptunnelname":<String_value>,

"vxlanvlanmap":<String_value>,

"targettd":<Integer_value>,

"msr":<String_value>,

"monitor":<String_value>,

"curstate":<Integer_value>,

"totalprobes":<Integer_value>,

"totalfailedprobes":<Integer_value>,

"failedprobes":<Integer_value>,

"monstatcode":<Integer_value>,
```

```
"monstatparam1":<Integer_value>,

"monstatparam2":<Integer_value>,

"monstatparam3":<Integer_value>,

"data":<Boolean_value>,

"ownergroup":<String_value>,

"pbrchildcount":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/nspbr/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/nspbr/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/nspbr/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of nspbr resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "nspbr": [ {

name:<String_value>,detail:<Boolean_value>"action":<String_value>,

"srcmac":<String_value>,

"srcmacmask":<String_value>,

"protocol":<String_value>,

"protocolnumber":<Integer_value>,

"srcportval":<String_value>,

"srcportdataset":<String_value>,

"srcportop":<String_value>,

"td":<Integer_value>,

"destportval":<String_value>,

"destportdataset":<String_value>,

"destportop":<String_value>,

"srcipval":<String_value>,

"srcipdataset":<String_value>,

"srcipop":<String_value>,

"destipval":<String_value>,

"destipop":<String_value>,

"destipdataset":<String_value>,
```

```
"vlan":<Integer_value>,

"vxlan":<Integer_value>,

"state":<String_value>,

"Interface":<String_value>,

"hits":<Integer_value>,

"priority":<Integer_value>,

"kernelstate":<String_value>,

"nexthopval":<String_value>,

"iptunnelname":<String_value>,

"vxlanvlanmap":<String_value>,

"targettd":<Integer_value>,

"msr":<String_value>,

"monitor":<String_value>,

"curstate":<Integer_value>,

"totalprobes":<Integer_value>,

"totalfailedprobes":<Integer_value>,

"failedprobes":<Integer_value>,

"monstatcode":<Integer_value>,

"monstatparam1":<Integer_value>,

"monstatparam2":<Integer_value>,

"monstatparam3":<Integer_value>,

"data":<Boolean_value>,
```

```
"ownergroup":<String_value>,

"pbrchildcount":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/nspbr? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nspbr": [ { "__count": "#no"} ] }
```

nspbr6

Configuration for PBR6 entry resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the PBR6. Must begin with an ASCII alphabetic or underscore \(_\) character, and must contain only ASCII alphanumeric, underscore, hash \(#\), period \(.\), space, colon \(:\), at \(@\), equals \(=\), and hyphen \(-\) characters. Cannot be changed after the PBR6 is created. Minimum length = 1
td	<Integer>	Read-write	Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0. Minimum value = 0 Maximum value = 4094
action	<String>	Read-write	Action to perform on the outgoing IPv6 packets that match the PBR6. Available settings function as follows:

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			* ALLOW - The Citrix ADC sends the packet to the designated next-hop router. * DENY - The Citrix ADC applies the routing table for normal destination-based routing. Possible values = ALLOW, DENY
srcipv6	<Boolean>	Read-write	IP address or range of IP addresses to match against the source IP address of an outgoing IPv6 packet. In the command line interface, separate the range with a hyphen.
srcipop	<String>	Read-write	Either the equals (=) or does not equal (!=) logical operator. Possible values = =, !=, EQ, NEQ
srcipv6val	<String>	Read-write	IP address or range of IP addresses to match against the source IP address of an outgoing IPv6 packet. In the command line interface, separate

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			the range with a hyphen.
srcport	<Boolean>	Read-write	Port number or range of port numbers to match against the source port number of an outgoing IPv6 packet. In the command line interface, separate the range with a hyphen. For example: 40-90.
srcportop	<String>	Read-write	Either the equals (=) or does not equal (!=) logical operator. Possible values = =, !=, EQ, NEQ
srcportval	<String>	Read-write	Source port (range). Maximum length = 65535
destipv6	<Boolean>	Read-write	IP address or range of IP addresses to match against the destination IP address of an outgoing IPv6 packet. In the command line interface, separate the range with a hyphen.
destipop	<String>	Read-write	Either the equals (=) or does not equal (!=) logical operator.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = =, !=, EQ, NEQ
destipv6val	<String>	Read-write	IP address or range of IP addresses to match against the destination IP address of an outgoing IPv6 packet. In the command line interface, separate the range with a hyphen.
destport	<Boolean>	Read-write	Port number or range of port numbers to match against the destination port number of an outgoing IPv6 packet. In the command line interface, separate the range with a hyphen. For example: 40-90. Note: The destination port can be specified only for TCP and UDP protocols.
destportop	<String>	Read-write	Either the equals (=) or does not equal (!=) logical operator. Possible values = =, !=, EQ, NEQ

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
destportval	<String>	Read-write	Destination port (range). Maximum length = 65535
srcmac	<String>	Read-write	MAC address to match against the source MAC address of an outgoing IPv6 packet.
srcmacmask	<String>	Read-write	Used to define range of Source MAC address. It takes string of 0 and 1, 0s are for exact match and 1s for wildcard. For matching first 3 bytes of MAC address, srcMacMask value "000000111111". . Default value: "000000000000"
protocol	<String>	Read-write	Protocol, identified by protocol name, to match against the protocol of an outgoing IPv6 packet. Possible values = ICMPV6, TCP, UDP, ICMP, IGMP, EGP, IGP, ARGUS, RDP, RSVP, EIGRP, L2TP, ISIS, GGP, IPoverIP, ST, CBT, BBN-RCC-M, NVP-

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			II, PUP, EMCON, XNET, CHAOS, MUX, DCN-MEAS, HMP, PRM, XNS-IDP, TRUNK-1, TRUNK-2, LEAF-1, LEAF-2, IRTP, ISO-TP4, NETBLT, MFE-NSP, MERIT-INP, SEP, 3PC, IDPR, XTP, DDP, IDPR-CMTP, TP++, IL, IPv6, SDRP, IPv6-Route, IPv6-Frag, IDRP, GRE, MHRP, BNA, ESP, AH, I-NLSP, SWIPE, NARP, MOBILE, TLSP, SKIP, IPv6-NoNx, IPv6-Opts, Any-Host-Internal-Protocol, CFTP, Any-Local-Network, SAT-EXPAK, KRYPTOLAN, RVD, IPPC, Any-Distributed-File-System, TFTP, VISA, IPCV, CPNX, CPHB, WSN, PVP, BR-SAT-MO, SUN-ND, WB-MON, WB-EXPAK, ISO-IP, VMTP, SECURE-VM, VINES, TTP,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			NSFNET-IG, DGP, TCF, OSPFIGP, Sprite-RP, LARP, MTP, AX.25, IPIP, MICP, SCC-SP, ETHERIP, Any-Private-Encryption-Scheme, GMTP, IFMP, PNNI, PIM, ARIS, SCPS, QNX, A/N, IPComp, SNP, Compaq-Pe, IPX-in-IP, VRRP, PGM, Any-0-Hop-Protocol, ENCAP, DDX, IATP, STP, SRP, UTI, SMP, SM, PTP, FIRE, CRTP, CRUDP, SSCOPMCE, IPLT, SPS, PIPE, SCTP, FC, RSVP-E2E-IGNORE, Mobility-Header, UDPLite
protocolnumber	<Integer>	Read-write	Protocol, identified by protocol number, to match against the protocol of an outgoing IPv6 packet. Minimum value = 1 Maximum value = 255

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
vlan	<Integer>	Read-write	ID of the VLAN. The Citrix ADC compares the PBR6 only to the outgoing packets on the specified VLAN. If you do not specify an interface ID, the appliance compares the PBR6 to the outgoing packets on all VLANs. Minimum value = 1 Maximum value = 4094
vxlan	<Integer>	Read-write	ID of the VXLAN. The Citrix ADC compares the PBR6 only to the outgoing packets on the specified VXLAN. If you do not specify an interface ID, the appliance compares the PBR6 to the outgoing packets on all VXLANs. Minimum value = 1 Maximum value = 16777215
Interface	<String>	Read-write	ID of an interface. The Citrix ADC compares the PBR6 only to the outgoing packets on the specified interface. If you do not specify a value, the appliance

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			compares the PBR6 to the outgoing packets on all interfaces.
priority	<Integer>	Read-write	Priority of the PBR6, which determines the order in which it is evaluated relative to the other PBR6s. If you do not specify priorities while creating PBR6s, the PBR6s are evaluated in the order in which they are created. Minimum value = 1 Maximum value = 81920
state	<String>	Read-write	Enable or disable the PBR6. After you apply the PBR6s, the Citrix ADC compares outgoing packets to the enabled PBR6s. Default value: ENABLED Possible values = ENABLED, DISABLED
msr	<String>	Read-write	Monitor the route specified by the Next Hop parameter. Default value: DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ENABLED, DISABLED
monitor	<String>	Read-write	The name of the monitor.(Can be only of type ping or ARP). Minimum length = 1
nexthop	<Boolean>	Read-write	IP address of the next hop router to which to send matching packets if action is set to ALLOW. This next hop should be directly reachable from the appliance.
nexthopval	<String>	Read-write	The Next Hop IPv6 address.
iptunnel	<String>	Read-write	The iptunnel name where packets need to be forwarded upon.
vxlanvlanmap	<String>	Read-write	The vlan to vxlan mapping to be applied for incoming packets over this pbr tunnel.
nexthopvlan	<Integer>	Read-write	VLAN number to be used for link local nexthop . Minimum value = 1 Maximum value = 4094

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ownergroup	<String>	Read-write	The owner node group in a Cluster for this pbr rule. If owner node group is not specified then the pbr rule is treated as Striped pbr rule. Default value: DEFAULT_NG Minimum length = 1
detail	<Boolean>	Read-write	To get a detailed view.
kernelstate	<String>	Read-only	Commit status of the PBR6. Default value: NOTAPPLIED Possible values = APPLIED, NOTAPPLIED, RE-APPLY, SFAPPLIED, SFNOTAPPLIED
hits	<Integer>	Read-only	Number of hits of this PBR6.
curstate	<Integer>	Read-only	If this route is UP/DOWN.
totalprobes	<Integer>	Read-only	The total number of probes sent.
totalfailedprobes	<Integer>	Read-only	The total number of failed probes.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
failedprobes	<Integer>	Read-only	Number of the current failed monitoring probes.
monstatcode	<Integer>	Read-only	The code indicating the monitor response.
monstatparam1	<Integer>	Read-only	First parameter for use with message code.
monstatparam2	<Integer>	Read-only	Second parameter for use with message code.
monstatparam3	<Integer>	Read-only	Third parameter for use with message code.
data	<Boolean>	Read-only	Internal data of this route.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- RENUMBER
- DELETE
- UPDATE
- UNSET
- ENABLE
- DISABLE
- GET (ALL)

- GET
- COUNT
- CLEAR
- APPLY

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/nspbr6 **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nspbr6":{

<b>"name":<String_value>,

</b>"td":<Integer_value>,

<b>"action":<String_value>,

</b>"srcipv6":<Boolean_value>,

"srcipop":<String_value>,

"srcipv6val":<String_value>,

"srcport":<Boolean_value>,

"srcportop":<String_value>,

"srcportval":<String_value>,

"destipv6":<Boolean_value>,

"destipop":<String_value>,

"destipv6val":<String_value>,

"destport":<Boolean_value>,

"destportop":<String_value>,

"destportval":<String_value>,

"srcmac":<String_value>,

"srcmacmask":<String_value>,

"protocol":<String_value>,

"protocolnumber":<Integer_value>,

"vlan":<Integer_value>,

"vxlan":<Integer_value>,
```

```
"Interface":<String_value>,

"priority":<Integer_value>,

"state":<String_value>,

"msr":<String_value>,

"monitor":<String_value>,

"nexthop":<Boolean_value>,

"nexthopval":<String_value>,

"iptunnel":<String_value>,

"vxlanvlanmap":<String_value>,

"nexthopvlan":<Integer_value>,

"ownergroup":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

RENUMBER

URL: http:// <netscaler-ip-address> /nitro/v1/config/nspbr6? **action=renumber HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nspbr6":{

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/nspbr6/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/nspbr6 **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nspbr6":{

<b>"name":<String_value>,

</b>"action":<String_value>,

"srcipv6":<Boolean_value>,

"srcipop":<String_value>,
```

```
"srcipv6val":<String_value>,

"srcport":<Boolean_value>,

"srcportop":<String_value>,

"srcportval":<String_value>,

"destipv6":<Boolean_value>,

"destipop":<String_value>,

"destipv6val":<String_value>,

"destport":<Boolean_value>,

"destportop":<String_value>,

"destportval":<String_value>,

"srcmac":<String_value>,

"srcmacmask":<String_value>,

"protocol":<String_value>,

"protocolnumber":<Integer_value>,

"vlan":<Integer_value>,

"vxlan":<Integer_value>,

"Interface":<String_value>,

"priority":<Integer_value>,

"msr":<String_value>,

"monitor":<String_value>,

"nexthop":<Boolean_value>,

"nexthopval":<String_value>,
```

```
"iptunnel":<String_value>,

"vxlanvlanmap":<String_value>,

"nexthopvlan":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/nspbr6? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nspbr6":{

<b>"name":<String_value>,

</b>"srcipv6":true,

"srcport":true,

"destipv6":true,

"destport":true,

"srcmac":true,

"srcmacmask":true,

"protocol":true,
```

```
"Interface":true,

"vlan":true,

"vxlan":true,

"msr":true,

"monitor":true,

"nexthop":true,

"iptunnel":true,

"nexthopvlan":true,

"vxlanvlanmap":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

ENABLE

URL: http:// <netscaler-ip-address> /nitro/v1/config/nspbr6? **action=enable HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nspbr6":{

<b>"name":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DISABLE

URL: http:// <netscaler-ip-address> /nitro/v1/config/nspbr6? **action=disable HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nspbr6":{

<b>"name":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

CLEAR

URL: http:// <netscaler-ip-address> /nitro/v1/config/nspbr6? **action=clear HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nspbr6":{

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

APPLY

URL: http:// <netscaler-ip-address> /nitro/v1/config/nspbr6? **action=apply HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nspbr6":{

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/nspbr6 **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/nspbr6? **args=name: <String_value> ,detail: <Boolean_value>**

Use this query-parameter to get nspbr6 resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/config/nspbr6? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/nspbr6? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of nspbr6 resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/nspbr6? **view=summary**

Use this query-parameter to get the summary output of nspbr6 resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/nspbr6? **pagesize=#no;pageno=#no**

Use this query-parameter to get the nspbr6 resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nspbr6": [ {

name:<String_value>,detail:<Boolean_value>"td":<Integer_value>,

"action":<String_value>,

"srcmac":<String_value>,

"srcmacmask":<String_value>,
```

```
"protocol":<String_value>,

"protocolnumber":<Integer_value>,

"srcportval":<String_value>,

"srcportop":<String_value>,

"destportval":<String_value>,

"destportop":<String_value>,

"srcipv6val":<String_value>,

"srcipop":<String_value>,

"destipv6val":<String_value>,

"destipop":<String_value>,

"vlan":<Integer_value>,

"vxlan":<Integer_value>,

"state":<String_value>,

"kernelstate":<String_value>,

"Interface":<String_value>,

"hits":<Integer_value>,

"priority":<Integer_value>,

"msr":<String_value>,

"monitor":<String_value>,

"curstate":<Integer_value>,

"totalprobes":<Integer_value>,

"totalfailedprobes":<Integer_value>,
```

```
"failedprobes":<Integer_value>,

"monstatcode":<Integer_value>,

"monstatparam1":<Integer_value>,

"monstatparam2":<Integer_value>,

"monstatparam3":<Integer_value>,

"nexthopval":<String_value>,

"iptunnel":<String_value>,

"vxlanvlanmap":<String_value>,

"nexthopvlan":<Integer_value>,

"data":<Boolean_value>,

"ownergroup":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/nspbr6/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/nspbr6/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/nspbr6/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of nspbr6 resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "nspbr6": [ {

name:<String_value>,detail:<Boolean_value>"td":<Integer_value>,

"action":<String_value>,

"srcmac":<String_value>,

"srcmacmask":<String_value>,

"protocol":<String_value>,

"protocolnumber":<Integer_value>,

"srcportval":<String_value>,

"srcportop":<String_value>,

"destportval":<String_value>,

"destportop":<String_value>,

"srcipv6val":<String_value>,

"srcipop":<String_value>,

"destipv6val":<String_value>,

"destipop":<String_value>,
```

```
"vlan":<Integer_value>,

"vxlan":<Integer_value>,

"state":<String_value>,

"kernelstate":<String_value>,

"Interface":<String_value>,

"hits":<Integer_value>,

"priority":<Integer_value>,

"msr":<String_value>,

"monitor":<String_value>,

"curstate":<Integer_value>,

"totalprobes":<Integer_value>,

"totalfailedprobes":<Integer_value>,

"failedprobes":<Integer_value>,

"monstatcode":<Integer_value>,

"monstatparam1":<Integer_value>,

"monstatparam2":<Integer_value>,

"monstatparam3":<Integer_value>,

"nexthopval":<String_value>,

"iptunnel":<String_value>,

"vxlanvlanmap":<String_value>,

"nexthopvlan":<Integer_value>,

"data":<Boolean_value>,
```

```
"ownergroup":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/nspbr6? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nspbr6": [ { "__count": "#no"} ] }
```

nspbrs

Configuration for Policy based routing resource.

Operations

- RENUMBER
- CLEAR
- APPLY

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

RENUMBER

URL: http:// <netscaler-ip-address> /nitro/v1/config/nspbrs? **action=renumber**

HTTP Method: POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nspbrs":{

}}
```

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

CLEAR

URL: http:// <netscaler-ip-address> /nitro/v1/config/nspbrs? **action=clear**

HTTP Method: POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nspbrs":{

}}
```

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

APPLY

URL: http:// <netscaler-ip-address> /nitro/v1/config/nspbrs? **action=apply**

HTTP Method: POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nspbrs":{

}}
```

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

nsratecontrol

Configuration for rate control resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
tcpthreshold	<Integer>	Read-write	Number of SYNs permitted per 10 milliseconds.
udpthreshold	<Integer>	Read-write	Number of UDP packets permitted per 10 milliseconds.
icmpthreshold	<Integer>	Read-write	Number of ICMP packets permitted per 10 milliseconds. Default value: 100
tcprstthreshold	<Integer>	Read-write	The number of TCP RST packets permitted per 10 milli

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			second. zero means rate control is disabled and 0xffffffff means every thing is rate controlled. Default value: 100
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- UPDATE
- UNSET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsratecontrol **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nsratecontrol":{

"tcpthreshold":<Integer_value>,

"udpthreshold":<Integer_value>,

"icmpthreshold":<Integer_value>,

"tcprstthreshold":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsratecontrol? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nsratecontrol":{

"tcpthreshold":true,

"udpthreshold":true,

"icmpthreshold":true,

"tcprstthreshold":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsratecontrol **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nsratecontrol": [ {

"tcpthreshold":<Integer_value>,

"udpthreshold":<Integer_value>,
```

```
"icmpthreshold":<Integer_value>,

"tcprstthreshold":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

nsrollbackcmd

Configuration for Generate rollback commands resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
filename	<String>	Read-write	File that contains the commands for which the rollback commands must be generated. Specify the full path of the file name.
outtype	<String>	Read-write	Format in which the rollback commands must be generated. Possible values = cli, xml
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsrollbackcmd **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/nsrollbackcmd? **args=filename: <String_value> ,outtype: <String_value>**

Use this query-parameter to get nsrollbackcmd resources based on additional properties.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nsrollbackcmd": [ {

filename:<String_value>,outtype:<String_value>"_nextgenapiresource":<Strin
g_value>

}]}
```

nsrpcnode

Configuration for rpc node resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ipaddress	<String>	Read-write	IP address of the node. This has to be in the same subnet as the NSIP address. Minimum length = 1
password	<String>	Read-write	Password to be used in authentication with the peer system node. Minimum length = 1
srcip	<String>	Read-write	Source IP address to be used to communicate with the peer system node. The default

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			value is 0, which means that the appliance uses the NSIP address as the source IP address.
secure	<String>	Read-write	State of the channel when talking to the node. Default value: YES Possible values = YES, NO
validatecert	<String>	Read-write	validate the server certificate for secure SSL connections. Default value: NO Possible values = YES, NO
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsrpcnode **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nsrpcnode":{

<b>"ipaddress":<String_value>,

</b>"password":<String_value>,

"srcip":<String_value>,
```

```
"secure":<String_value>,

"validatecert":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsrpcnode? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nsrpcnode":{

<b>"ipaddress":<String_value>,

</b>"srcip":true,

"secure":true,

"validatecert":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsrpcnode **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/nsrpcnode? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/nsrpcnode? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of nsrpcnode resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/nsrpcnode? **view=summary**

Use this query-parameter to get the summary output of nsrpcnode resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/nsrpcnode? **pagesize=#no;pageno=#no**

Use this query-parameter to get the nsrpcnode resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nsrpcnode": [ {

"ipaddress":<String_value>,
```

```
"password":<String_value>,

"srcip":<String_value>,

"secure":<String_value>,

"validatecert":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsrpcnode/ ipaddress_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/nsrpcnode/ ipaddress_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/nsrpcnode/ ipaddress_value<String> ? **view=summary**

Use this query-parameter to get the summary output of nsrpcnode resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "nsrpcnode": [ {

"ipaddress":<String_value>,

"password":<String_value>,

"srcip":<String_value>,

"secure":<String_value>,

"validatecert":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsrpcnode? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nsrpcnode": [ { "__count": "#no"} ] }
```

nsrunningconfig

Configuration for running configuration resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
withdefaults	<Boolean>	Read-write	Include default values of parameters that have not been explicitly configured. If this argument is disabled, such parameters are not included.
response	<String>	Read-only	running config data as text blob.
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsrunningconfig

Query-parameters:

args

http:// <netscaler-ip-address> /nitro/v1/config/nsrunningconfig? **args=withdefaults: <Boolean_value>**

Use this query-parameter to get nsrunningconfig resources based on additional properties.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nsrunningconfig": [ {

withdefaults:<Boolean_value>"response":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

nssavedconfig

Configuration for last saved configuration resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
textblob	<String>	Read-write	Text of the last saved configuration.
_nextgenapiresource	<String>	Read-write	.

Operations

(click to see Properties)

- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/nssavedconfig

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nssavedconfig": [ {

"textblob":<String_value>,
```

```
"_nextgenapiresource":<String_value>

}]}
```

nsservicefunction

Configuration for service Function resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
servicefunctionname	<String>	Read-write	Name of the service function to be created. Leading character must be a number or letter. Other characters allowed, after the first character, are @ _ - . (period) : (colon) # and space ( ). Minimum length = 1
ingressvlan	<Integer>	Read-write	VLAN ID on which the traffic from service function reaches Citrix ADC. Minimum value = 1 Maximum value = 4094
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- UPDATE
- DELETE
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsservicefunction **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nsservicefunction":{

<b>"servicefunctionname":<String_value>,

</b><b>"ingressvlan":<Integer_value>

</b>}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsservicefunction **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nsservicefunction":{

<b>"servicefunctionname":<String_value>,

</b>"ingressvlan":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/nservicefunction/ servicefunctionname_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/nservicefunction **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/nservicefunction? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/nservicefunction? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of nservicefunction resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/nservicefunction? **view=summary**

Use this query-parameter to get the summary output of nservicefunction resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/nservicefunction? **pagesize=#no;pageno=#no**

Use this query-parameter to get the nservicefunction resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nsservicefunction": [ {

"servicefunctionname":<String_value>,

"ingressvlan":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsservicefunction/ servicefunctionname_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/nsservicefunction/ servicefunctionname_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/nsservicefunction/ servicefunctionname_value<String> ? **view=summary**

Use this query-parameter to get the summary output of nsservicefunction resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "nsservicefunction": [ {

"servicefunctionname":<String_value>,

"ingressvlan":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsservicefunction? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nsservicefunction": [ { "__count": "#no"} ] }
```

nsservicepath

Configuration for service Chain resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
servicepathname	<String>	Read-write	Name for the Service path. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Minimum length = 1
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsservicepath **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nsservicepath":{

<b>"servicepathname":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsservicepath/ servicepathname_value<String>
HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsservicepath **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/nsservicepath? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/nsservicepath? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of nsservicepath resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/nsservicepath? **view=summary**

Use this query-parameter to get the summary output of nsservicepath resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/nsservicepath? **pagesize=#no;pageno=#no**

Use this query-parameter to get the nsservicepath resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nsservicepath": [ {

"servicepathname":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsservicepath/ servicepathname_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/nsservicepath/ servicepathname_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/nsservicepath/ servicepathname_value<String> ? **view=summary**

Use this query-parameter to get the summary output of nsservicepath resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "nsservicepath": [ {

"servicepathname":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsservicepath? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nsservicepath": [ { "__count": "#no"} ] }
```

nsservicepath_binding

Binding object which returns the resources bound to nsservicepath.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
servicepathname	<String>	Read-write	Name for the Service path. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Minimum length = 1
nsservicepath_nsservicefunction_binding	<nsservicepath_nsservicefunction_binding []>	Read-only	nsservicefunction that can be bound to nsservicepath.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsservicepath_binding/servicepathname_value<String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nsservicepath_binding": [ {

"servicepathname":<String_value>,

"nsservicepath_nsservicefunction_binding":<nsservicepath_nsservicefunction
_binding[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsservicepath_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/nsservicepath_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nsservicepath_binding": [ {

"servicepathname":<String_value>,

"nsservicepath_nsservicefunction_binding":<nsservicepath_nsservicefunction
_binding[]_value>

}]}
```

nsservicepath_nsservicefunction_binding

Binding object showing the nsservicefunction that can be bound to nsservicepath.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
index	<Integer>	Read-write	The serviceindex of each servicefunction in path. Minimum value = 1
servicefunction	<String>	Read-write	List of service functions constituting the chain. Minimum length = 1
servicepathname	<String>	Read-write	Name for the Service path. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			(#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Minimum length = 1
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/nsservicepath_nsservicefunction_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"nsservicepath_nsservicefunction_binding":{

<b>"servicepathname":<String_value>,

</b><b>"servicefunction":<String_value>,

</b><b>"index":<Integer_value></b>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsservicepath_nsservicefunction_binding/ servicepathname_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/ config/nsservicepath_nsservicefunction_binding/ servicepathname_value<String> ? **args= servicefunction:<String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsservicepath_nsservicefunction_binding/ servicepathname_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/ config/nsservicepath_nsservicefunction_binding/ servicepathname_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of nsservicepath_nsservicefunction_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ nsservicepath_nsservicefunction_binding/ servicepathname_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the nsservicepath_nsservicefunction_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "nsservicepath_nsservicefunction_binding": [ {

"index":<Integer_value>,

"servicefunction":<String_value>,

"servicepathname":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsservicepath_nsservicefunction_binding
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/nsservicepath_nsservicefunction_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "nsservicepath_nsservicefunction_binding": [ {

"index":<Integer_value>,
```

```
"servicefunction":<String_value>,

"servicepathname":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsservicepath_nsservicefunction_binding/servicepathname_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"nsservicepath_nsservicefunction_binding": [ { "__count": "#no"} ] }
```

nssimpleacl

Configuration for simple ACL resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
aclname	<String>	Read-write	Name for the simple ACL rule. Must begin

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the simple ACL rule is created. Minimum length = 1
aclaction	<String>	Read-write	Drop incoming IPv4 packets that match the simple ACL rule. Possible values = DENY
td	<Integer>	Read-write	Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0. Minimum value = 0 Maximum value = 4094

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
srcip	<String>	Read-write	IP address to match against the source IP address of an incoming IPv4 packet.
destport	<Integer>	Read-write	Port number to match against the destination port number of an incoming IPv4 packet. DestPort is mandatory while setting Protocol. Omitting the port number and protocol creates an all-ports and all protocols simple ACL rule, which matches any port and any protocol. In that case, you cannot create another simple ACL rule specifying a specific port and the same source IPv4 address. Minimum value = 1 Maximum value = 65535
protocol	<String>	Read-write	Protocol to match against the protocol

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			of an incoming IPv4 packet. You must set this parameter if you have set the Destination Port parameter. Possible values = TCP, UDP
ttl	<Integer>	Read-write	Number of seconds, in multiples of four, after which the simple ACL rule expires. If you do not want the simple ACL rule to expire, do not specify a TTL value. Minimum value = 4 Maximum value = 2147483647
estsessions	<Boolean>	Read-write	.
hits	<Integer>	Read-only	Number of hits for this ACL rule.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- CLEAR
- DELETE
- FLUSH
- GET (ALL)

- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/nssimpleacl **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nssimpleacl":{

<b>"aclname":<String_value>,

</b><b>"aclaction":<String_value>,

</b>"td":<Integer_value>,

<b>"srcip":<String_value>,

</b>"destport":<Integer_value>,

"protocol":<String_value>,

"ttl":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

CLEAR

URL: http:// <netscaler-ip-address> /nitro/v1/config/nssimpleacl? **action=clear HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nssimpleacl":{

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/nssimpleacl/ aclname_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

FLUSH

URL: http:// <netscaler-ip-address> /nitro/v1/config/nssimpleacl? **action=flush HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nssimpleacl":{

<b>"estsessions":<Boolean_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/nssimpleacl **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/nssimpleacl? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/nssimpleacl? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of nssimpleacl resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/nssimpleacl? **view=summary**

Use this query-parameter to get the summary output of nssimpleacl resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/nssimpleacl? **pagesize=#no;pageno=#no**

Use this query-parameter to get the nssimpleacl resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nssimpleacl": [ {

"aclname":<String_value>,

"aclaction":<String_value>,
```

```
"td":<Integer_value>,

"srcip":<String_value>,

"destport":<Integer_value>,

"protocol":<String_value>,

"ttl":<Integer_value>,

"hits":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/nssimpleacl/ aclname_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/nssimpleacl/ aclname_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/nssimpleacl/ aclname_value<String> ? **view=summary**

Use this query-parameter to get the summary output of nssimpleacl resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "nssimpleacl": [ {

"aclname":<String_value>,

"aclaction":<String_value>,

"td":<Integer_value>,

"srcip":<String_value>,

"destport":<Integer_value>,

"protocol":<String_value>,

"ttl":<Integer_value>,

"hits":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/nssimpleacl? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nssimpleacl": [ { "__count": "#no"} ] }
```

nssimpleacl6

Configuration for simple ACL6 resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
aclname	<String>	Read-write	Name for the simple ACL6 rule. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the simple ACL6 rule is created. Minimum length = 1
td	<Integer>	Read-write	Integer value that uniquely identifies the traffic domain in

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0. Minimum value = 0 Maximum value = 4094
aclaction	<String>	Read-write	Drop incoming IPv6 packets that match the simple ACL6 rule. Possible values = DENY
srcipv6	<String>	Read-write	IP address to match against the source IP address of an incoming IPv6 packet.
destport	<Integer>	Read-write	Port number to match against the destination port number of an incoming IPv6 packet. DestPort is mandatory while setting Protocol. Omitting the port number and protocol creates an all-ports and all protocol simple

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			ACL6 rule, which matches any port and any protocol. In that case, you cannot create another simple ACL6 rule specifying a specific port and the same source IPv6 address. Minimum value = 1 Maximum value = 65535
protocol	<String>	Read-write	Protocol to match against the protocol of an incoming IPv6 packet. You must set this parameter if you set the Destination Port parameter. Possible values = TCP, UDP
ttl	<Integer>	Read-write	Number of seconds, in multiples of four, after which the simple ACL6 rule expires. If you do not want the simple ACL6 rule to expire, do not specify a TTL value. Minimum value = 4

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum value = 2147483647
estsessions	<Boolean>	Read-write	.
hits	<Integer>	Read-only	Number of hits for this SACL6 rule.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- CLEAR
- FLUSH
- DELETE
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/nssimpleacl6 **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nssimpleacl6":{

<b>"aclname":<String_value>,

</b>"td":<Integer_value>,

<b>"aclaction":<String_value>,

</b><b>"srcipv6":<String_value>,

</b>"destport":<Integer_value>,

"protocol":<String_value>,

"ttl":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

CLEAR

URL: http:// <netscaler-ip-address> /nitro/v1/config/nssimpleacl6? **action=clear HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nssimpleacl6":{

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

FLUSH

URL: http:// <netscaler-ip-address> /nitro/v1/config/nssimpleacl6? **action=flush HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nssimpleacl6":{

<b>"estsessions":<Boolean_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/nssimpleacl6/ aclname_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/nssimpleacl6 **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/nssimpleacl6? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/nssimpleacl6? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of nssimpleacl6 resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/nssimpleacl6? **view=summary**

Use this query-parameter to get the summary output of nssimpleacl6 resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/nssimpleacl6? **pagesize=#no;pageno=#no**

Use this query-parameter to get the nssimpleacl6 resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nssimpleacl6": [ {

"aclname":<String_value>,

"aclaction":<String_value>,

"td":<Integer_value>,

"srcipv6":<String_value>,

"destport":<Integer_value>,

"protocol":<String_value>,

"ttl":<Integer_value>,

"hits":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/nssimpleacl6/ aclname_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/nssimpleacl6/ aclname_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/nssimpleacl6/ aclname_value<String> ? **view=summary**

Use this query-parameter to get the summary output of nssimpleacl6 resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "nssimpleacl6": [ {

"aclname":<String_value>,

"aclaction":<String_value>,

"td":<Integer_value>,

"srcipv6":<String_value>,
```

```
"destport":<Integer_value>,

"protocol":<String_value>,

"ttl":<Integer_value>,

"hits":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/nssimpleacl6? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nssimpleacl6": [ { "__count": "#no"} ] }
```

nssourceroutecachetable

Configuration for Source IP Mac Cache Table. resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
sourceip	<String>	Read-write	Source ip of the connection.
sourcemac	<String>	Read-write	source MAC address of an incoming IPv6 packet.
vlan	<Integer>	Read-write	ID of the VLAN.
Interface	<String>	Read-write	ID of an interface.
_nextgenapiresource	<String>	Read-write	.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- GET (ALL)
- COUNT
- FLUSH

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

FLUSH

URL: http:// <netscaler-ip-address> /nitro/v1/config/nssourceroutecachetable? **action=flush**

HTTP Method: POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nssourceroutecachetable":{

}}
```

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/nssourceroutecachetable

Query-parameters:

attrs

http:// <netscaler-ip-address> /nitro/v1/config/nssourceroutecachetable? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter

http:// <netscaler-ip-address> /nitro/v1/config/nssourceroutecachetable? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of nssourceroutecachetable resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view

http:// <netscaler-ip-address> /nitro/v1/config/nssourceroutecachetable? **view=summary**

Use this query-parameter to get the summary output of nssourceroutecachetable resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination

http:// <netscaler-ip-address> /nitro/v1/config/nssourceroutecachetable? **pagesize=#no;pageno=#no**

Use this query-parameter to get the nssourceroutecachetable resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nssourceroutecachetable": [ {

"sourceip":<String_value>,

"sourcemac":<String_value>,

"vlan":<Integer_value>,

"Interface":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/nssourceroutecachetable? **count=yes**

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nssourceroutecachetable": [ { "__count": "#no"} ] }
```

nsspparams

Configuration for Surge Protection parameter resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
basethreshold	<Integer>	Read-write	Maximum number of server connections that can be opened before surge protection is activated. Default value: 200 Minimum value = 0 Maximum value = 32767
throttle	<String>	Read-write	Rate at which the system opens connections to the server. Default value: Normal Possible values = Aggressive, Normal, Relaxed
table0	<Integer[]>	Read-only	Table.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
builtin	<String[]>	Read-only	Flag to determine if sp param is built-in or not. Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL
feature	<String>	Read-only	The feature to be checked while applying this config.
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- UPDATE
- UNSET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.
- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsspparams **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nsspparams":{

"basethreshold":<Integer_value>,

"throttle":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsspparams? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nsspparams":{

"basethreshold":true,

"throttle":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsspparams **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nsspparams": [ {

"basethreshold":<Integer_value>,
```

```
"throttle":<String_value>,

"table0":<Integer[]_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

nsstats

Configuration for stats resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
cleanuplevel	<String>	Read-write	The level of stats to be cleared. 'global' option will clear global counters only, 'all' option will clear all device counters also along with global counters. For both the cases only 'ever incrementing counters' i.e. total counters will be cleared. Possible values = global, all

Operations

(click to see Properties)

- CLEAR

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

CLEAR

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsstats? **action=clear HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nsstats":{

<b>"cleanuplevel":<String_value>
```

```
</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

nssurgeq

Configuration for surge queue resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of a virtual server, service or service group for which the SurgeQ must be flushed.
servername	<String>	Read-write	Name of a service group member. This argument is needed when you want to flush the SurgeQ of a service group.
port	<Integer>	Read-write	port on which server is bound to the entity(Servicegroup). Range 1 - 65535 * in CLI is represented as 65535 in NITRO API

Operations

(click to see Properties)

- FLUSH

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

FLUSH

URL: http:// <netscaler-ip-address> /nitro/v1/config/nssurgeq? **action=flush HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nssurgeq":{

"name":<String_value>,

"servername":<String_value>,

"port":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

nstcpbufparam

Configuration for tcp buffer parameter resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
size	<Integer>	Read-write	TCP buffering size per connection, in kilobytes. Default value: 64 Minimum value = 4 Maximum value = 20480
memlimit	<Integer>	Read-write	Maximum memory, in megabytes, that can be used for buffering. Default value: 64

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
builtin	<String[]>	Read-only	Flag to determine if TCP buffering is built-in or not. Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL
feature	<String>	Read-only	The feature to be checked while applying this config.
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- UPDATE
- UNSET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.
- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/nstcpbufparam **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nstcpbufparam":{

"size":<Integer_value>,

"memlimit":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/nstcpbufparam? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nstcpbufparam":{

"size":true,

"memlimit":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/nstcpbufparam **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nstcpbufparam": [ {

"size":<Integer_value>,
```

```
"memlimit":<Integer_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

nstcpparam

Configuration for tcp parameters resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ws	<String>	Read-write	Enable or disable window scaling. Default value: ENABLED Possible values = ENABLED, DISABLED
wsval	<Integer>	Read-write	Factor used to calculate the new window size. This argument is needed only when the window scaling is enabled. Default value: 8 Minimum value = 0

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum value = 14
sack	<String>	Read-write	Enable or disable Selective ACKnowledgement (SACK). Default value: ENABLED Possible values = ENABLED, DISABLED
learnvsvrmss	<String>	Read-write	Enable or disable maximum segment size (MSS) learning for virtual servers. Default value: DISABLED Possible values = ENABLED, DISABLED
maxburst	<Integer>	Read-write	Maximum number of TCP segments allowed in a burst. Default value: 6 Minimum value = 1 Maximum value = 255
initialcwnd	<Integer>	Read-write	Initial maximum upper limit on the number of TCP packets that can be outstanding on the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			TCP link to the server. Default value: 10 Minimum value = 1 Maximum value = 44
recvbuffsize	<Integer>	Read-write	TCP Receive buffer size. Default value: 8190 Minimum value = 8190 Maximum value = 20971520
delayedack	<Integer>	Read-write	Timeout for TCP delayed ACK, in milliseconds. Default value: 100 Minimum value = 10 Maximum value = 300
downstaterst	<String>	Read-write	Flag to switch on RST on down services. Default value: DISABLED Possible values = ENABLED, DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
nagle	<String>	Read-write	Enable or disable the Nagle algorithm on TCP connections. Default value: DISABLED Possible values = ENABLED, DISABLED
limitedpersist	<String>	Read-write	Limit the number of persist (zero window) probes. Default value: ENABLED Possible values = ENABLED, DISABLED
oooqsize	<Integer>	Read-write	Maximum size of out-of-order packets queue. A value of 0 means no limit. Default value: 300 Minimum value = 0 Maximum value = 65535
ackonpush	<String>	Read-write	Send immediate positive acknowledgement (ACK) on receipt of TCP packets with PUSH flag. Default value: ENABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ENABLED, DISABLED
maxpktpermss	<Integer>	Read-write	Maximum number of TCP packets allowed per maximum segment size (MSS). Minimum value = 0 Maximum value = 1460
pktperretx	<Integer>	Read-write	Maximum limit on the number of packets that should be retransmitted on receiving a partial ACK. Default value: 1 Minimum value = 1 Maximum value = 100
minrto	<Integer>	Read-write	Minimum retransmission timeout, in milliseconds, specified in 10-millisecond increments (value must yield a whole number if divided by 10). Default value: 1000 Minimum value = 10

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum value = 64000
slowstartincr	<Integer>	Read-write	Multiplier that determines the rate at which slow start increases the size of the TCP transmission window after each acknowledgement of successful transmission. Default value: 2 Minimum value = 1 Maximum value = 100
maxdynserverprobes	<Integer>	Read-write	Maximum number of probes that Citrix ADC can send out in 10 milliseconds, to dynamically learn a service. Citrix ADC probes for the existence of the origin in case of wildcard virtual server or services. Default value: 7 Minimum value = 1 Maximum value = 65535
synholdfastgiveup	<Integer>	Read-write	Maximum threshold. After crossing this threshold number of

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			outstanding probes for origin, the Citrix ADC reduces the number of connection retries for probe connections. Default value: 1024 Minimum value = 256 Maximum value = 65535
maxsynholdperprobe	<Integer>	Read-write	Limit the number of client connections (SYN) waiting for status of single probe. Any new SYN packets will be dropped. Default value: 128 Minimum value = 1 Maximum value = 255
maxsynhold	<Integer>	Read-write	Limit the number of client connections (SYN) waiting for status of probe system wide. Any new SYN packets will be dropped. Default value: 16384 Minimum value = 256

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum value = 65535
msslearninterval	<Integer>	Read-write	Duration, in seconds, to sample the Maximum Segment Size (MSS) of the services. The Citrix ADC determines the best MSS to set for the virtual server based on this sampling. The argument to enable maximum segment size (MSS) for virtual servers must be enabled. Default value: 180 Minimum value = 1 Maximum value = 1048576
msslearndelay	<Integer>	Read-write	Frequency, in seconds, at which the virtual servers learn the Maximum segment size (MSS) from the services. The argument to enable maximum segment size (MSS) for virtual servers must be enabled. Default value: 3600 Minimum value = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum value = 1048576
maxtimewaitconn	<Integer>	Read-write	Maximum number of connections to hold in the TCP TIME_WAIT state on a packet engine. New connections entering TIME_WAIT state are proactively cleaned up. Default value: 7000 Minimum value = 1
kaprobeupdatelastactivity	<String>	Read-write	Update last activity for KA probes. Default value: ENABLED Possible values = ENABLED, DISABLED
maxsynackretx	<Integer>	Read-write	When 'syncookie' is disabled in the TCP profile that is bound to the virtual server or service, and the number of TCP SYN+ACK retransmission by Citrix ADC for that virtual server or service crosses this threshold, the Citrix ADC responds by using the TCP SYN-Cookie mechanism.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: 100 Minimum value = 100 Maximum value = 1048576
synattackdetection	<String>	Read-write	Detect TCP SYN packet flood and send an SNMP trap. Default value: ENABLED Possible values = ENABLED, DISABLED
connflushifnomem	<String>	Read-write	Flush an existing connection if no memory can be obtained for new connection. HALF_CLOSED_AND_IDLE: Flush a connection that is closed by us but not by peer, or failing that, a connection that is past configured idle time. New connection fails if no such connection can be found. FIFO: If no half-closed or idle connection can be

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			found, flush the oldest non-management connection, even if it is active. New connection fails if the oldest few connections are management connections. Note: If you enable this setting, you should also consider lowering the zombie timeout and half-close timeout, while setting the Citrix ADC timeout. See Also: connFlushThres argument below. Default value: NSA_CONNFLUSH_NONE Possible values = NONE , HALFCLOSED_AND_IDLE, FIFO
connflushthres	<Integer>	Read-write	Flush an existing connection (as configured through -connFlushIfNoMem

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			FIFO) if the system has more than specified number of connections, and a new connection is to be established. Note: This value may be rounded down to be a whole multiple of the number of packet engines running. Minimum value = 1
mptcpconcloseonpassivesf	<String>	Read-write	Accept DATA_FIN/ FAST_CLOSE on passive subflow. Default value: ENABLED Possible values = ENABLED, DISABLED
mptcpchecksum	<String>	Read-write	Use MPTCP DSS checksum. Default value: ENABLED Possible values = ENABLED, DISABLED
mptcpsftimeout	<Integer>	Read-write	The timeout value in seconds for idle mptcp subflows. If this timeout is not set, idle subflows are cleared after cltTimeout of vserver.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: 0 Minimum value = 0 Maximum value = 31536000
mptcpsfreplacetimeout	<Integer>	Read-write	The minimum idle time value in seconds for idle mptcp subflows after which the sublow is replaced by new incoming subflow if maximum subflow limit is reached. The priority for replacement is given to those subflow without any transaction. Default value: 10 Minimum value = 0 Maximum value = 31536000
mptcpmaxsf	<Integer>	Read-write	Maximum number of subflow connections supported in established state per mptcp connection. Default value: 4 Minimum value = 2 Maximum value = 6
mptcpmaxpendingsf	<Integer>	Read-write	Maximum number of subflow connections supported in pending

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			join state per mptcp connection. Default value: 4 Minimum value = 0 Maximum value = 4
mptcppendingjointhreshold	<Integer>	Read-write	Maximum system level pending join connections allowed. Default value: 0 Minimum value = 0 Maximum value = 4294967294
mptcprtostoswitchsf	<Integer>	Read-write	Number of RTO's at subflow level, after which MPCTP should start using other subflow. Default value: 2 Minimum value = 1 Maximum value = 6
mptcpusebackupondss	<String>	Read-write	When enabled, if NS receives a DSS on a backup subflow, NS will start using that subflow to send data. And if disabled, NS will continue to transmit on current chosen subflow. In case there is some error on a subflow (like RTO's/RST etc.) then NS can choose

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			a backup subflow irrespective of this tunable. Default value: ENABLED Possible values = ENABLED, DISABLED
tcpmaxretries	<Integer>	Read-write	Number of RTO's after which a connection should be freed. Default value: 7 Minimum value = 1 Maximum value = 7
mptcpimmediatesfcloseonfin	<String>	Read-write	Allow subflows to close immediately on FIN before the DATA_FIN exchange is completed at mptcp level. Default value: DISABLED Possible values = ENABLED, DISABLED
mptcpclosemptcpsessiononlastsfclose	<String>	Read-write	Allow to send DATA FIN or FAST CLOSE on mptcp connection while sending FIN or RST on the last subflow.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: DISABLED Possible values = ENABLED, DISABLED
mptcpsendsfresetoption	<String>	Read-write	Allow MPTCP subflows to send TCP RST Reason (MP_TCPRST) Option while sending TCP RST. Default value: DISABLED Possible values = ENABLED, DISABLED
mptcpfastcloseoption	<String>	Read-write	Allow to select option ACK or RESET to force the closure of an MPTCP connection abruptly. Default value: ACK Possible values = ACK, RESET
mptcpreliableaddaddr	<String>	Read-write	If enabled, Citrix ADC retransmits MPTCP ADD-ADDR option if echo response is not received within the timeout interval. The retransmission is attempted only once.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: DISABLED Possible values = ENABLED, DISABLED
tcpfastopencookietimeout	<Integer>	Read-write	Timeout in seconds after which a new TFO Key is computed for generating TFO Cookie. If zero, the same key is used always. If timeout is less than 120seconds, NS defaults to 120seconds timeout. Default value: 0 Minimum value = 0 Maximum value = 31536000
autosyncookietimeout	<Integer>	Read-write	Timeout for the server to function in syncookie mode after the synattack. This is valid if TCP syncookie is disabled on the profile and server acts in non syncookie mode by default. Default value: 30 Minimum value = 7

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum value = 65535
tcpfintimeout	<Integer>	Read-write	The amount of time in seconds, after which a TCP connnection in the TCP TIME-WAIT state is flushed. Default value: 40 Minimum value = 10 Maximum value = 240
compacttcpoptionnoop	<String>	Read-write	If enabled, non-negotiated TCP options are removed from the received packet while proxying it. By default, non-negotiated TCP options would be replaced by NOPs in the proxied packets. This option is not applicable for Citrix ADC generated packets. Default value: DISABLED Possible values = ENABLED, DISABLED
delinkclientserveronrst	<String>	Read-write	If enabled, Delink client and server connection, when

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			there is outstanding data to be sent to the other side. Default value: DISABLED Possible values = ENABLED, DISABLED
rfc5961chlgacklimit	<Integer>	Read-write	Limits number of Challenge ACK sent per second, as recommended in RFC 5961(Improving TCP's Robustness to Blind In-Window Attacks). Default value: 0 Minimum value = 0 Maximum value = 2147483647
enhancedisngeneration	<String>	Read-write	If enabled, increase the ISN variation in SYN-ACKs sent by the NetScaler. Default value: DISABLED Possible values = ENABLED, DISABLED
sendresetreasoncode	<String>	Read-write	If enabled, NetScaler includes a debug code indicating the reason for the reset in the TCP Window

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			header field of outgoing TCP RST segments. Default value: DISABLED Possible values = ENABLED, DISABLED
builtin	<String[]>	Read-only	Flag to determine if the tcp param is built-in or not. Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL
feature	<String>	Read-only	The feature to be checked while applying this config.
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- UPDATE
- UNSET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/nstcpparam **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nstcpparam":{

"ws":<String_value>,

"wsval":<Integer_value>,

"sack":<String_value>,

"learnvsvrmss":<String_value>,

"maxburst":<Integer_value>,

"initialcwnd":<Integer_value>,
```

```
"recvbuffsize":<Integer_value>,

"delayedack":<Integer_value>,

"downstaterst":<String_value>,

"nagle":<String_value>,

"limitedpersist":<String_value>,

"oooqsize":<Integer_value>,

"ackonpush":<String_value>,

"maxpktpermss":<Integer_value>,

"pktperretx":<Integer_value>,

"minrto":<Integer_value>,

"slowstartincr":<Integer_value>,

"maxdynserverprobes":<Integer_value>,

"synholdfastgiveup":<Integer_value>,

"maxsynholdperprobe":<Integer_value>,

"maxsynhold":<Integer_value>,

"msslearninterval":<Integer_value>,

"msslearndelay":<Integer_value>,

"maxtimewaitconn":<Integer_value>,

"kaprobeupdatelastactivity":<String_value>,

"maxsynackretx":<Integer_value>,

"synattackdetection":<String_value>,

"connflushifnomem":<String_value>,
```

```
"connflushthres":<Integer_value>,

"mptcpconcloseonpassivesf":<String_value>,

"mptcpchecksum":<String_value>,

"mptcpsftimeout":<Integer_value>,

"mptcpsfreplacetimeout":<Integer_value>,

"mptcpmaxsf":<Integer_value>,

"mptcpmaxpendingsf":<Integer_value>,

"mptcppendingjointhreshold":<Integer_value>,

"mptcprtostoswitchsf":<Integer_value>,

"mptcpusebackupondss":<String_value>,

"tcpmaxretries":<Integer_value>,

"mptcpimmediatesfcloseonfin":<String_value>,

"mptcpclosemptcpsessiononlastsfclose":<String_value>,

"mptcpsendsfresetoption":<String_value>,

"mptcpfastcloseoption":<String_value>,

"mptcpreliableaddaddr":<String_value>,

"tcpfastopencookietimeout":<Integer_value>,

"autosyncookietimeout":<Integer_value>,

"tcpfintimeout":<Integer_value>,

"compacttcpoptionnoop":<String_value>,

"delinkclientserveronrst":<String_value>,

"rfc5961chlgacklimit":<Integer_value>,
```

```
"enhancedisngeneration":<String_value>,

"sendresetreasoncode":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/nstcpparam? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nstcpparam":{

"ws":true,

"wsval":true,

"sack":true,

"learnvsvrmss":true,

"maxburst":true,

"initialcwnd":true,

"recvbuffsize":true,

"delayedack":true,
```

```
"downstaterst":true,

"nagle":true,

"limitedpersist":true,

"oooqsize":true,

"ackonpush":true,

"maxpktpermss":true,

"pktperretx":true,

"minrto":true,

"slowstartincr":true,

"maxdynserverprobes":true,

"synholdfastgiveup":true,

"maxsynholdperprobe":true,

"maxsynhold":true,

"msslearninterval":true,

"msslearndelay":true,

"maxtimewaitconn":true,

"kaprobeupdatelastactivity":true,

"maxsynackretx":true,

"synattackdetection":true,

"connflushifnomem":true,

"connflushthres":true,

"mptcpconcloseonpassivesf":true,
```

```
"mptcpchecksum":true,

"mptcpsftimeout":true,

"mptcpsfreplacetimeout":true,

"mptcpmaxsf":true,

"mptcpmaxpendingsf":true,

"mptcppendingjointhreshold":true,

"mptcprtostoswitchsf":true,

"mptcpusebackupondss":true,

"tcpmaxretries":true,

"mptcpimmediatesfcloseonfin":true,

"mptcpclosemptcpsessiononlastsfclose":true,

"mptcpsendsfresetoption":true,

"mptcpfastcloseoption":true,

"mptcpreliableaddaddr":true,

"tcpfastopencookietimeout":true,

"autosyncookietimeout":true,

"tcpfintimeout":true,

"compacttcpoptionnoop":true,

"delinkclientserveronrst":true,

"rfc5961chlgacklimit":true,

"enhancedisngeneration":true,

"sendresetreasoncode":true
```

```
}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/nstcpparam **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nstcpparam": [ {

"ws":<String_value>,

"wsval":<Integer_value>,

"sack":<String_value>,

"learnvsvrmss":<String_value>,

"maxburst":<Integer_value>,

"initialcwnd":<Integer_value>,

"recvbuffsize":<Integer_value>,
```

```
"delayedack":<Integer_value>,

"downstaterst":<String_value>,

"nagle":<String_value>,

"limitedpersist":<String_value>,

"oooqsize":<Integer_value>,

"ackonpush":<String_value>,

"maxpktpermss":<Integer_value>,

"pktperretx":<Integer_value>,

"minrto":<Integer_value>,

"slowstartincr":<Integer_value>,

"maxdynserverprobes":<Integer_value>,

"synholdfastgiveup":<Integer_value>,

"maxsynholdperprobe":<Integer_value>,

"maxsynhold":<Integer_value>,

"msslearninterval":<Integer_value>,

"msslearndelay":<Integer_value>,

"maxtimewaitconn":<Integer_value>,

"kaprobeupdatelastactivity":<String_value>,

"maxsynackretx":<Integer_value>,

"synattackdetection":<String_value>,

"connflushifnomem":<String_value>,

"connflushthres":<Integer_value>,
```

```
"mptcpconcloseonpassivesf":<String_value>,

"mptcpchecksum":<String_value>,

"mptcpsftimeout":<Integer_value>,

"mptcpsfreplacetimeout":<Integer_value>,

"mptcpmaxsf":<Integer_value>,

"mptcpmaxpendingsf":<Integer_value>,

"mptcppendingjointhreshold":<Integer_value>,

"mptcprtostoswitchsf":<Integer_value>,

"mptcpusebackupondss":<String_value>,

"tcpmaxretries":<Integer_value>,

"mptcpimmediatesfcloseonfin":<String_value>,

"mptcpclosemptcpsessiononlastsfclose":<String_value>,

"mptcpsendsfresetoption":<String_value>,

"mptcpfastcloseoption":<String_value>,

"mptcpreliableaddaddr":<String_value>,

"tcpfastopencookietimeout":<Integer_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"autosyncookietimeout":<Integer_value>,

"tcpfintimeout":<Integer_value>,

"compacttcpoptionnoop":<String_value>,

"delinkclientserveronrst":<String_value>,
```

```
"rfc5961chlgacklimit":<Integer_value>,

"enhancedisngeneration":<String_value>,

"sendresetreasoncode":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

nstcpprofile

Configuration for TCP profile resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for a TCP profile. Must begin with a letter, number, or the underscore \(_\) character. Other characters allowed, after the first character, are the hyphen \(-\), period \(.\), hash \(#\), space \(\), at \(@\), colon \(:\), and equal \(=\) characters. The name of a TCP profile cannot be changed after it is created. CLI Users: If the name includes one or more spaces, enclose the name in

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			double or single quotation marks \ (for example, "my tcp profile" or 'my tcp profile'\). Minimum length = 1 Maximum length = 127
ws	<String>	Read-write	Enable or disable window scaling. Default value: ENABLED Possible values = ENABLED, DISABLED
sack	<String>	Read-write	Enable or disable Selective ACKnowledgement (SACK). Default value: ENABLED Possible values = ENABLED, DISABLED
wsval	<Integer>	Read-write	Factor used to calculate the new window size. This argument is needed only when window scaling is enabled.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: TCP_DEFAULT_WSVAL Minimum value = 0 Maximum value = 14
nagle	<String>	Read-write	Enable or disable the Nagle algorithm on TCP connections. Default value: DISABLED Possible values = ENABLED, DISABLED
ackonpush	<String>	Read-write	Send immediate positive acknowledgement (ACK) on receipt of TCP packets with PUSH flag. Default value: ENABLED Possible values = ENABLED, DISABLED
mss	<Integer>	Read-write	Maximum number of octets to allow in a TCP data segment. Default value: TCP_DEFAULT_CLIENT_MSS

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum value = 0 Maximum value = 9176
maxburst	<Integer>	Read-write	Maximum number of TCP segments allowed in a burst. Default value: 6 Minimum value = 1 Maximum value = 255
initialcwnd	<Integer>	Read-write	Initial maximum upper limit on the number of TCP packets that can be outstanding on the TCP link to the server. Default value: TCP_DEFAULT_INITIALCWND Minimum value = 1 Maximum value = 44
delayedack	<Integer>	Read-write	Timeout for TCP delayed ACK, in milliseconds. Default value: 100 Minimum value = 10 Maximum value = 300

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
oooqsize	<Integer>	Read-write	Maximum size of out-of-order packets queue. A value of 0 means no limit. Default value: TCP_DEFAULT_MAX_OOO_PKTS Minimum value = 0 Maximum value = 65535
maxpktpermss	<Integer>	Read-write	Maximum number of TCP packets allowed per maximum segment size (MSS). Minimum value = 0 Maximum value = 1460
pktperretx	<Integer>	Read-write	Maximum limit on the number of packets that should be retransmitted on receiving a partial ACK. Default value: 1 Minimum value = 1 Maximum value = 512
minrto	<Integer>	Read-write	Minimum retransmission timeout, in milliseconds, specified in 10-millisecond

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			increments (value must yield a whole number if divided by 10). Default value: 1000 Minimum value = 10 Maximum value = 64000
slowstartincr	<Integer>	Read-write	Multiplier that determines the rate at which slow start increases the size of the TCP transmission window after each acknowledgement of successful transmission. Default value: 2 Minimum value = 1 Maximum value = 100
buffersize	<Integer>	Read-write	TCP buffering size, in bytes. Default value: TCP_DEFAULT_BUFFSIZE Minimum value = 8190 Maximum value = 20971520

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
syncookie	<String>	Read-write	Enable or disable the SYNCOOKIE mechanism for TCP handshake with clients. Disabling SYNCOOKIE prevents SYN attack protection on the Citrix ADC. Default value: ENABLED Possible values = ENABLED, DISABLED
kaprobeupdatelastactivity	<String>	Read-write	Update last activity for the connection after receiving keep-alive (KA) probes. Default value: ENABLED Possible values = ENABLED, DISABLED
flavor	<String>	Read-write	Set TCP congestion control algorithm. Default value: BIC Possible values = Default, Westwood, BIC, CUBIC, Nile, BBR
dynamicreceivebuffering	<String>	Read-write	Enable or disable dynamic receive buffering. When enabled, allows the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			receive buffer to be adjusted dynamically based on memory and network conditions. Note: The buffer size argument must be set for dynamic adjustments to take place. Default value: DISABLED Possible values = ENABLED, DISABLED
ka	<String>	Read-write	Send periodic TCP keep-alive (KA) probes to check if peer is still up. Default value: DISABLED Possible values = ENABLED, DISABLED
kaconnidletime	<Integer>	Read-write	Duration, in seconds, for the connection to be idle, before sending a keep-alive (KA) probe. Minimum value = 1 Maximum value = 4095

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
kamaxprobes	<Integer>	Read-write	Number of keep-alive (KA) probes to be sent when not acknowledged, before assuming the peer to be down. Minimum value = 1 Maximum value = 254
kaprobeinterval	<Integer>	Read-write	Time interval, in seconds, before the next keep-alive (KA) probe, if the peer does not respond. Minimum value = 1 Maximum value = 4095
sendbuffsize	<Integer>	Read-write	TCP Send Buffer Size. Default value: TCP_DEFAULT_SENDBUFFSIZE Minimum value = 8190 Maximum value = 20971520
mptcp	<String>	Read-write	Enable or disable Multipath TCP. Default value: DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ENABLED, DISABLED
establishclientconn	<String>	Read-write	Establishing Client Client connection on First data/ Final-ACK / Automatic. Default value: AUTOMATIC Possible values = AUTOMATIC, CONN_ESTABLISHED, ON_FIRST_DATA
tcpsegoffload	<String>	Read-write	Offload TCP segmentation to the NIC. If set to AUTOMATIC, TCP segmentation will be offloaded to the NIC, if the NIC supports it. Default value: AUTOMATIC Possible values = AUTOMATIC, DISABLED
rfc5961compliance	<String>	Read-write	Enable or disable RFC 5961 compliance to protect against tcp spoofing(RST/SYN/Data). When enabled, will be

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			compliant with RFC 5961. Default value: DISABLED Possible values = ENABLED, DISABLED
rstwindowattenuate	<String>	Read-write	Enable or disable RST window attenuation to protect against spoofing. When enabled, will reply with corrective ACK when a sequence number is invalid. Default value: DISABLED Possible values = ENABLED, DISABLED
rstmaxack	<String>	Read-write	Enable or disable acceptance of RST that is out of window yet echoes highest ACK sequence number. Useful only in proxy mode. Default value: DISABLED Possible values = ENABLED, DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
spoofsyndrop	<String>	Read-write	Enable or disable drop of invalid SYN packets to protect against spoofing. When disabled, established connections will be reset when a SYN packet is received. Default value: ENABLED Possible values = ENABLED, DISABLED
ecn	<String>	Read-write	Enable or disable TCP Explicit Congestion Notification. Default value: DISABLED Possible values = ENABLED, DISABLED
mptcpdropdataonpreestsf	<String>	Read-write	Enable or disable silently dropping the data on Pre-Established subflow. When enabled, DSS data packets are dropped silently instead of dropping the connection when data is received on pre established subflow.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: DISABLED Possible values = ENABLED, DISABLED
mptcpfastopen	<String>	Read-write	Enable or disable Multipath TCP fastopen. When enabled, DSS data packets are accepted before receiving the third ack of SYN handshake. Default value: DISABLED Possible values = ENABLED, DISABLED
mptcpsessiontimeout	<Integer>	Read-write	MPTCP session timeout in seconds. If this value is not set, idle MPTCP sessions are flushed after vserver's client idle timeout. Default value: 0 Minimum value = 0 Maximum value = 86400
timestamp	<String>	Read-write	Enable or Disable TCP Timestamp option (RFC 1323).

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: DISABLED Possible values = ENABLED, DISABLED
dsack	<String>	Read-write	Enable or disable DSACK. Default value: ENABLED Possible values = ENABLED, DISABLED
ackaggregation	<String>	Read-write	Enable or disable ACK Aggregation. Default value: DISABLED Possible values = ENABLED, DISABLED
frto	<String>	Read-write	Enable or disable FRTO (Forward RTO-Recovery). Default value: ENABLED Possible values = ENABLED, DISABLED
maxcwnd	<Integer>	Read-write	TCP Maximum Congestion Window. Default value: 524288

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum value = 8190 Maximum value = 20971520
fack	<String>	Read-write	Enable or disable FACK (Forward ACK). Default value: ENABLED Possible values = ENABLED, DISABLED
tcpmode	<String>	Read-write	TCP Optimization modes TRANSPARENT / ENDPOINT. Default value: TRANSPARENT Possible values = TRANSPARENT, ENDPOINT
tcpfastopen	<String>	Read-write	Enable or disable TCP Fastopen. When enabled, NS can receive or send Data in SYN or SYN-ACK packets. Default value: DISABLED Possible values = ENABLED, DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
hystart	<String>	Read-write	Enable or disable CUBIC Hystart. Default value: DISABLED Possible values = ENABLED, DISABLED
dupackthresh	<Integer>	Read-write	TCP dupack threshold. Default value: 3 Minimum value = 1 Maximum value = 15
burstratecontrol	<String>	Read-write	TCP Burst Rate Control DISABLED/FIXED/DYNAMIC. FIXED requires a TCP rate to be set. Default value: DISABLED Possible values = DISABLED, FIXED, DYNAMIC
tcprate	<Integer>	Read-write	TCP connection payload send rate in Kb/s. Default value: 0 Minimum value = 0 Maximum value = 10000000

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
rateqmax	<Integer>	Read-write	Maximum connection queue size in bytes, when BurstRateControl is used. Default value: 0 Minimum value = 0 Maximum value = 1000000000
drophalfclosedconnontimeout	<String>	Read-write	Silently drop tcp half closed connections on idle timeout. Default value: DISABLED Possible values = ENABLED, DISABLED
dropestconnontimeout	<String>	Read-write	Silently drop tcp established connections on idle timeout. Default value: DISABLED Possible values = ENABLED, DISABLED
applyadaptivetcp	<String>	Read-write	Apply Adaptive TCP optimizations. Default value: DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ENABLED, DISABLED
tcpfastopencookiesize	<Integer>	Read-write	TCP FastOpen Cookie size. This accepts only even numbers. Odd number is trimmed down to nearest even number. Default value: 8 Minimum value = 4 Maximum value = 16
taillossprobe	<String>	Read-write	TCP tail loss probe optimizations. Default value: DISABLED Possible values = ENABLED, DISABLED
clientiptcpoption	<String>	Read-write	Client IP in TCP options. Default value: DISABLED Possible values = ENABLED, DISABLED
clientiptcpoptionnumber	<Integer>	Read-write	ClientIP TCP Option number.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: DISABLED Minimum value = 1 Maximum value = 254
mpcapablecbit	<String>	Read-write	Set C bit in MP-CAPABLE Syn-Ack sent by Citrix ADC. Default value: DISABLED Possible values = ENABLED, DISABLED
sendclientportintcpoption	<String>	Read-write	Send Client Port number along with Client IP in TCP-Options. ClientIpTcpOption must be ENABLED. Default value: DISABLED Possible values = ENABLED, DISABLED
slowstartthreshold	<Integer>	Read-write	TCP Slow Start Threhsold Value. Default value: 524288 Minimum value = 8190

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum value = 20971520
refcnt	<Integer>	Read-only	Number of entities using this profile.
builtin	<String[]>	Read-only	Flag to determine if tcp profile is built-in or not. Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL
feature	<String>	Read-only	The feature to be checked while applying this config.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/nstcpprofile **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nstcpprofile":{

<b>"name":<String_value>,

</b>"ws":<String_value>,

"sack":<String_value>,
```

```
"wsval":<Integer_value>,

"nagle":<String_value>,

"ackonpush":<String_value>,

"mss":<Integer_value>,

"maxburst":<Integer_value>,

"initialcwnd":<Integer_value>,

"delayedack":<Integer_value>,

"oooqsize":<Integer_value>,

"maxpktpermss":<Integer_value>,

"pktperretx":<Integer_value>,

"minrto":<Integer_value>,

"slowstartincr":<Integer_value>,

"buffersize":<Integer_value>,

"syncookie":<String_value>,

"kaprobeupdatelastactivity":<String_value>,

"flavor":<String_value>,

"dynamicreceivebuffering":<String_value>,

"ka":<String_value>,

"kaconnidletime":<Integer_value>,

"kamaxprobes":<Integer_value>,

"kaprobeinterval":<Integer_value>,

"sendbuffsize":<Integer_value>,
```

```
"mptcp":<String_value>,

"establishclientconn":<String_value>,

"tcpsegoffload":<String_value>,

"rfc5961compliance":<String_value>,

"rstwindowattenuate":<String_value>,

"rstmaxack":<String_value>,

"spoofsyndrop":<String_value>,

"ecn":<String_value>,

"mptcpdropdataonpreestsf":<String_value>,

"mptcpfastopen":<String_value>,

"mptcpsessiontimeout":<Integer_value>,

"timestamp":<String_value>,

"dsack":<String_value>,

"ackaggregation":<String_value>,

"frto":<String_value>,

"maxcwnd":<Integer_value>,

"fack":<String_value>,

"tcpmode":<String_value>,

"tcpfastopen":<String_value>,

"hystart":<String_value>,

"dupackthresh":<Integer_value>,

"burstratecontrol":<String_value>,
```

```
"tcprate":<Integer_value>,

"rateqmax":<Integer_value>,

"drophalfclosedconnontimeout":<String_value>,

"dropestconnontimeout":<String_value>,

"applyadaptivetcp":<String_value>,

"tcpfastopencookiesize":<Integer_value>,

"taillossprobe":<String_value>,

"clientiptcpoption":<String_value>,

"clientiptcpoptionnumber":<Integer_value>,

"mpcapablecbit":<String_value>,

"sendclientportintcpoption":<String_value>,

"slowstartthreshold":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/nstcpprofile/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/nstcpprofile **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nstcpprofile":{

<b>"name":<String_value>,

</b>"ws":<String_value>,

"sack":<String_value>,

"wsval":<Integer_value>,

"nagle":<String_value>,

"ackonpush":<String_value>,

"mss":<Integer_value>,

"maxburst":<Integer_value>,

"initialcwnd":<Integer_value>,

"delayedack":<Integer_value>,

"oooqsize":<Integer_value>,

"maxpktpermss":<Integer_value>,

"pktperretx":<Integer_value>,

"minrto":<Integer_value>,
```

```
"slowstartincr":<Integer_value>,

"buffersize":<Integer_value>,

"syncookie":<String_value>,

"kaprobeupdatelastactivity":<String_value>,

"flavor":<String_value>,

"dynamicreceivebuffering":<String_value>,

"ka":<String_value>,

"kaconnidletime":<Integer_value>,

"kamaxprobes":<Integer_value>,

"kaprobeinterval":<Integer_value>,

"sendbuffsize":<Integer_value>,

"mptcp":<String_value>,

"establishclientconn":<String_value>,

"tcpsegoffload":<String_value>,

"rfc5961compliance":<String_value>,

"rstwindowattenuate":<String_value>,

"rstmaxack":<String_value>,

"spoofsyndrop":<String_value>,

"ecn":<String_value>,

"mptcpdropdataonpreestsf":<String_value>,

"mptcpfastopen":<String_value>,

"mptcpsessiontimeout":<Integer_value>,
```

```
"timestamp":<String_value>,

"dsack":<String_value>,

"ackaggregation":<String_value>,

"frto":<String_value>,

"maxcwnd":<Integer_value>,

"fack":<String_value>,

"tcpmode":<String_value>,

"tcpfastopen":<String_value>,

"hystart":<String_value>,

"dupackthresh":<Integer_value>,

"burstratecontrol":<String_value>,

"tcprate":<Integer_value>,

"rateqmax":<Integer_value>,

"drophalfclosedconnontimeout":<String_value>,

"dropestconnontimeout":<String_value>,

"applyadaptivetcp":<String_value>,

"tcpfastopencookiesize":<Integer_value>,

"taillossprobe":<String_value>,

"clientiptcpoption":<String_value>,

"clientiptcpoptionnumber":<Integer_value>,

"mpcapablecbit":<String_value>,

"sendclientportintcpoption":<String_value>,
```

```
"slowstartthreshold":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/nstcpprofile? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nstcpprofile":{

<b>"name":<String_value>,

</b>"ws":true,

"sack":true,

"wsval":true,

"nagle":true,

"ackonpush":true,

"mss":true,

"maxburst":true,

"initialcwnd":true,
```

```
"delayedack":true,

"oooqsize":true,

"maxpktpermss":true,

"pktperretx":true,

"minrto":true,

"slowstartincr":true,

"buffersize":true,

"syncookie":true,

"kaprobeupdatelastactivity":true,

"flavor":true,

"dynamicreceivebuffering":true,

"ka":true,

"kamaxprobes":true,

"kaconnidletime":true,

"kaprobeinterval":true,

"sendbuffsize":true,

"mptcp":true,

"establishclientconn":true,

"tcpsegoffload":true,

"rfc5961compliance":true,

"rstwindowattenuate":true,

"rstmaxack":true,
```

```
"spoofsyndrop":true,

"ecn":true,

"mptcpdropdataonpreestsf":true,

"mptcpfastopen":true,

"mptcpsessiontimeout":true,

"timestamp":true,

"dsack":true,

"ackaggregation":true,

"frto":true,

"maxcwnd":true,

"fack":true,

"tcpmode":true,

"tcpfastopen":true,

"hystart":true,

"dupackthresh":true,

"burstratecontrol":true,

"tcprate":true,

"rateqmax":true,

"drophalfclosedconnontimeout":true,

"dropestconnontimeout":true,

"applyadaptivetcp":true,

"clientiptcpoption":true,
```

```
"mpcapablecbit":true,

"slowstartthreshold":true,

"tcpfastopencookiesize":true,

"taillossprobe":true,

"clientiptcpoptionnumber":true,

"sendclientportintcpoption":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/nstcpprofile **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/nstcpprofile? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/nstcpprofile? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of nstcpprofile resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/nstcpprofile? **view=summary**

Use this query-parameter to get the summary output of nstcpprofile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/nstcpprofile? **pagesize=#no;pageno=#no**

Use this query-parameter to get the nstcpprofile resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nstcpprofile": [ {

"name":<String_value>,

"ws":<String_value>,

"sack":<String_value>,

"wsval":<Integer_value>,

"nagle":<String_value>,

"ackonpush":<String_value>,

"mss":<Integer_value>,

"maxburst":<Integer_value>,

"initialcwnd":<Integer_value>,

"delayedack":<Integer_value>,

"oooqsize":<Integer_value>,

"maxpktpermss":<Integer_value>,
```

```
"pktperretx":<Integer_value>,

"minrto":<Integer_value>,

"slowstartincr":<Integer_value>,

"buffersize":<Integer_value>,

"flavor":<String_value>,

"refcnt":<Integer_value>,

"syncookie":<String_value>,

"kaprobeupdatelastactivity":<String_value>,

"dynamicreceivebuffering":<String_value>,

"ka":<String_value>,

"kaconnidletime":<Integer_value>,

"kamaxprobes":<Integer_value>,

"kaprobeinterval":<Integer_value>,

"sendbuffsize":<Integer_value>,

"mptcp":<String_value>,

"establishclientconn":<String_value>,

"tcpsegoffload":<String_value>,

"rfc5961compliance":<String_value>,

"rstwindowattenuate":<String_value>,

"rstmaxack":<String_value>,

"timestamp":<String_value>,

"spoofsyndrop":<String_value>,
```

```
"ecn":<String_value>,

"mptcpdropdataonpreestsf":<String_value>,

"mptcpfastopen":<String_value>,

"mptcpsessiontimeout":<Integer_value>,

"dsack":<String_value>,

"ackaggregation":<String_value>,

"frto":<String_value>,

"maxcwnd":<Integer_value>,

"fack":<String_value>,

"tcpmode":<String_value>,

"tcpfastopen":<String_value>,

"hystart":<String_value>,

"dupackthresh":<Integer_value>,

"burstratecontrol":<String_value>,

"tcprate":<Integer_value>,

"rateqmax":<Integer_value>,

"drophalfclosedconnontimeout":<String_value>,

"dropestconnontimeout":<String_value>,

"applyadaptivetcp":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"tcpfastopencookiesize":<Integer_value>,
```

```
"taillossprobe":<String_value>,

"clientiptcpoption":<String_value>,

"clientiptcpoptionnumber":<Integer_value>,

"mpcapablecbit":<String_value>,

"sendclientportintcpoption":<String_value>,

"slowstartthreshold":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/nstcpprofile/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/nstcpprofile/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/nstcpprofile/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of nstcpprofile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "nstcpprofile": [ {

"name":<String_value>,

"ws":<String_value>,

"sack":<String_value>,

"wsval":<Integer_value>,

"nagle":<String_value>,

"ackonpush":<String_value>,

"mss":<Integer_value>,

"maxburst":<Integer_value>,

"initialcwnd":<Integer_value>,

"delayedack":<Integer_value>,

"oooqsize":<Integer_value>,

"maxpktpermss":<Integer_value>,

"pktperretx":<Integer_value>,

"minrto":<Integer_value>,

"slowstartincr":<Integer_value>,

"buffersize":<Integer_value>,
```

```
"flavor":<String_value>,

"refcnt":<Integer_value>,

"syncookie":<String_value>,

"kaprobeupdatelastactivity":<String_value>,

"dynamicreceivebuffering":<String_value>,

"ka":<String_value>,

"kaconnidletime":<Integer_value>,

"kamaxprobes":<Integer_value>,

"kaprobeinterval":<Integer_value>,

"sendbuffsize":<Integer_value>,

"mptcp":<String_value>,

"establishclientconn":<String_value>,

"tcpsegoffload":<String_value>,

"rfc5961compliance":<String_value>,

"rstwindowattenuate":<String_value>,

"rstmaxack":<String_value>,

"timestamp":<String_value>,

"spoofsyndrop":<String_value>,

"ecn":<String_value>,

"mptcpdropdataonpreestsf":<String_value>,

"mptcpfastopen":<String_value>,

"mptcpsessiontimeout":<Integer_value>,
```

```
"dsack":<String_value>,

"ackaggregation":<String_value>,

"frto":<String_value>,

"maxcwnd":<Integer_value>,

"fack":<String_value>,

"tcpmode":<String_value>,

"tcpfastopen":<String_value>,

"hystart":<String_value>,

"dupackthresh":<Integer_value>,

"burstratecontrol":<String_value>,

"tcprate":<Integer_value>,

"rateqmax":<Integer_value>,

"drophalfclosedconnontimeout":<String_value>,

"dropestconnontimeout":<String_value>,

"applyadaptivetcp":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"tcpfastopencookiesize":<Integer_value>,

"taillossprobe":<String_value>,

"clientiptcpoption":<String_value>,

"clientiptcpoptionnumber":<Integer_value>,

"mpcapablecbit":<String_value>,
```

```
"sendclientportintcpoption":<String_value>,

"slowstartthreshold":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/nstcpprofile? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nstcpprofile": [ { "__count": "#no"} ] }
```

nstestlicense

Configuration for testlicense resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
wl	<Boolean>	Read-write	Web Logging.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
sp	<Boolean>	Read-write	Surge Protection.
lb	<Boolean>	Read-write	Load Balancing.
cs	<Boolean>	Read-write	Content Switching.
cr	<Boolean>	Read-write	Cache Redirect.
cmp	<Boolean>	Read-write	Compression.
delta	<Boolean>	Read-write	Delta Compression.
ssl	<Boolean>	Read-write	Secure Sockets Layer.
gslb	<Boolean>	Read-write	Global Server Load Balancing.
gslbp	<Boolean>	Read-write	GSLB Proximity.
routing	<Boolean>	Read-write	Routing.
cf	<Boolean>	Read-write	Content Filter.
contentaccelerator	<Boolean>	Read-write	transparent Integrated Caching.
ic	<Boolean>	Read-write	Integrated Caching.
sslvpn	<Boolean>	Read-write	SSL VPN.
f_sslvpn_users	<Integer>	Read-write	Number of licensed users allowed by this license.
f_ica_users	<Integer>	Read-write	Number of licensed users allowed by ICAONLY license. As long as the AG Feature is licensed,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			unlimited number of ICA connections are accepted. (In API, 0 value for this parameter means unlimited when AG license in ON).
aaa	<Boolean>	Read-write	AAA.
ospf	<Boolean>	Read-write	OSPF Routing.
rip	<Boolean>	Read-write	RIP Routing.
bgp	<Boolean>	Read-write	BGP Routing.
rewrite	<Boolean>	Read-write	Rewrite.
ipv6pt	<Boolean>	Read-write	IPv6 protocol translation.
appfw	<Boolean>	Read-write	Application Firewall.
responder	<Boolean>	Read-write	Responder.
agee	<Boolean>	Read-write	.
nsxn	<Boolean>	Read-write	.
modelid	<Integer>	Read-write	Model Number ID. Represents different numbers for two types of licenses.: * Bandwidth licenses - specifies the throughput

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			bandwidth licensed for this appliance e.g. (For 20 Gbps) Model Number ID: 20000 * vCPU licenses - specifies number of vCPUs licensed for this appliance. e.g. (For 4 vCPU) Model Number ID: 4 vCPUs.
push	<Boolean>	Read-write	Citrix ADC Push.
appflow	<Boolean>	Read-write	AppFlow.
cloudbridge	<Boolean>	Read-write	CloudBridge.
cloudbridgeappliance	<Boolean>	Read-write	.
cloudextenderappliance	<Boolean>	Read-write	.
isis	<Boolean>	Read-write	ISIS Routing.
cluster	<Boolean>	Read-write	Clustering.
ch	<Boolean>	Read-write	Call Home.
appqoe	<Boolean>	Read-write	AppQoS.
appflowica	<Boolean>	Read-write	Appflow for ICA.
isstandardlic	<Boolean>	Read-write	Standard License.
isenterpriselic	<Boolean>	Read-write	Enterprise License.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
isplatinumlic	<Boolean>	Read-write	Platinum License.
issgwylic	<Boolean>	Read-write	Simple Gateway License.
isswglic	<Boolean>	Read-write	Secure Web Gateway License.
feo	<Boolean>	Read-write	Front End Optimization.
lsn	<Boolean>	Read-write	Large Scale NAT.
licensingmode	<String>	Read-write	Pooled Licensed. Default value: Local Possible values = Local, Pooled, Fips-Pooled, CICO, Fips-CICO, EXPRESS, CPU, CPU-Local, Self Managed Pool, Self Managed vCPU, LAS, LAS (Fixed Bandwidth)
daystoexpiration	<Integer>	Read-write	Days to expire. Minimum value = 0 Maximum value = 4294967294
rdpproxy	<Boolean>	Read-write	RDPPROXY.
rep	<Boolean>	Read-write	Reputation Services.
urlfiltering	<Boolean>	Read-write	URL Filtering.
videooptimization	<Boolean>	Read-write	Video Optimization.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
forwardproxy	<Boolean>	Read-write	Forward Proxy.
sslinterception	<Boolean>	Read-write	SSL Interception.
remotecontentinspection	<Boolean>	Read-write	Remote Content Inspection.
adaptivetcp	<Boolean>	Read-write	Adaptive TCP.
cqa	<Boolean>	Read-write	Connection Quality Analytics.
bot	<Boolean>	Read-write	Bot Management.
apigateway	<Boolean>	Read-write	API Gateway.
_nextgenapiresource	<String>	Read-write	.

Operations

(click to see Properties)

- GET (ALL)
- APPLY

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

APPLY

URL: http:// <netscaler-ip-address> /nitro/v1/config/nstestlicense? **action=apply HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nstestlicense":{

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/nstestlicense **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nstestlicense": [ {

"wl":<Boolean_value>,

"sp":<Boolean_value>,

"lb":<Boolean_value>,

"cs":<Boolean_value>,

"cr":<Boolean_value>,

"cmp":<Boolean_value>,

"delta":<Boolean_value>,

"ssl":<Boolean_value>,

"gslb":<Boolean_value>,

"gslbp":<Boolean_value>,

"routing":<Boolean_value>,

"cf":<Boolean_value>,

"contentaccelerator":<Boolean_value>,

"ic":<Boolean_value>,

"sslvpn":<Boolean_value>,

"f_sslvpn_users":<Integer_value>,
```

```
"f_ica_users":<Integer_value>,

"aaa":<Boolean_value>,

"ospf":<Boolean_value>,

"rip":<Boolean_value>,

"bgp":<Boolean_value>,

"rewrite":<Boolean_value>,

"ipv6pt":<Boolean_value>,

"appfw":<Boolean_value>,

"responder":<Boolean_value>,

"agee":<Boolean_value>,

"nsxn":<Boolean_value>,

"modelid":<Integer_value>,

"push":<Boolean_value>,

"appflow":<Boolean_value>,

"cloudbridge":<Boolean_value>,

"cloudbridgeappliance":<Boolean_value>,

"cloudextenderappliance":<Boolean_value>,

"isis":<Boolean_value>,

"cluster":<Boolean_value>,

"ch":<Boolean_value>,

"appqoe":<Boolean_value>,

"appflowica":<Boolean_value>,
```

```
"isstandardlic":<Boolean_value>,

"isenterpriselic":<Boolean_value>,

"isplatinumlic":<Boolean_value>,

"issgwylic":<Boolean_value>,

"isswglic":<Boolean_value>,

"feo":<Boolean_value>,

"lsn":<Boolean_value>,

"licensingmode":<String_value>,

"daystoexpiration":<Integer_value>,

"rdpproxy":<Boolean_value>,

"rep":<Boolean_value>,

"urlfiltering":<Boolean_value>,

"videooptimization":<Boolean_value>,

"forwardproxy":<Boolean_value>,

"sslinterception":<Boolean_value>,

"remotecontentinspection":<Boolean_value>,

"adaptivetcp":<Boolean_value>,

"cqa":<Boolean_value>,

"bot":<Boolean_value>,

"apigateway":<Boolean_value>,

"_nextgenapiresource":<String_value>

}]}
```

nstimeout

Configuration for timeout resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
zombie	<Integer>	Read-write	Interval, in seconds, at which the Citrix ADC zombie cleanup process must run. This process cleans up inactive TCP connections. Default value: 120 Minimum value = 1 Maximum value = 600
client	<Integer>	Read-write	Client idle timeout (in seconds). If zero, the service-type default value is taken when service is created. Default value: 0 Minimum value = 0 Maximum value = 18000
server	<Integer>	Read-write	Server idle timeout (in seconds). If zero, the service-type default value is taken when service is created.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: 0 Minimum value = 0 Maximum value = 18000
httpclient	<Integer>	Read-write	Global idle timeout, in seconds, for client connections of HTTP service type. This value is over ridden by the client timeout that is configured on individual entities. Default value: 0 Minimum value = 0 Maximum value = 18000
httpserver	<Integer>	Read-write	Global idle timeout, in seconds, for server connections of HTTP service type. This value is over ridden by the server timeout that is configured on individual entities. Default value: 0 Minimum value = 0 Maximum value = 18000
tcpclient	<Integer>	Read-write	Global idle timeout, in seconds, for non-HTTP client connections of TCP

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			service type. This value is over ridden by the client timeout that is configured on individual entities. Default value: 0 Minimum value = 0 Maximum value = 18000
tcpserver	<Integer>	Read-write	Global idle timeout, in seconds, for non-HTTP server connections of TCP service type. This value is over ridden by the server timeout that is configured on entities. Default value: 0 Minimum value = 0 Maximum value = 18000
anyclient	<Integer>	Read-write	Global idle timeout, in seconds, for non-TCP client connections. This value is over ridden by the client timeout that is configured on individual entities. Default value: 0 Minimum value = 0

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum value = 31536000
anyserver	<Integer>	Read-write	Global idle timeout, in seconds, for non TCP server connections. This value is over ridden by the server timeout that is configured on individual entities. Default value: 0 Minimum value = 0 Maximum value = 31536000
anytcpclient	<Integer>	Read-write	Global idle timeout, in seconds, for TCP client connections. This value takes precedence over entity level timeout settings (vserver/service). This is applicable only to transport protocol TCP. Default value: 0 Minimum value = 0 Maximum value = 31536000
anytcpserver	<Integer>	Read-write	Global idle timeout, in seconds, for TCP server connections. This value takes precedence over

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			entity level timeout settings (vserver/ service). This is applicable only to transport protocol TCP. Default value: 0 Minimum value = 0 Maximum value = 31536000
halfclose	<Integer>	Read-write	Idle timeout, in seconds, for connections that are in TCP half-closed state. Default value: 10 Minimum value = 1 Maximum value = 600
nontcpzombie	<Integer>	Read-write	Interval at which the zombie clean-up process for non-TCP connections should run. Inactive IP NAT connections will be cleaned up. Default value: 60 Minimum value = 1 Maximum value = 600
reducedfintimeout	<Integer>	Read-write	Alternative idle timeout, in seconds, for closed TCP

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			NATPCB connections. Default value: 30 Minimum value = 1 Maximum value = 300
reducedrsttimeout	<Integer>	Read-write	Timer interval, in seconds, for abruptly terminated TCP NATPCB connections. Default value: 0 Minimum value = 0 Maximum value = 300
newconnidletimeout	<Integer>	Read-write	Timer interval, in seconds, for new TCP NATPCB connections on which no data was received. Default value: 4 Minimum value = 1 Maximum value = 120
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- UPDATE
- UNSET

- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/nstimeout **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nstimeout":{

"zombie":<Integer_value>,
```

```
"client":<Integer_value>,

"server":<Integer_value>,

"httpclient":<Integer_value>,

"httpserver":<Integer_value>,

"tcpclient":<Integer_value>,

"tcpserver":<Integer_value>,

"anyclient":<Integer_value>,

"anyserver":<Integer_value>,

"anytcpclient":<Integer_value>,

"anytcpserver":<Integer_value>,

"halfclose":<Integer_value>,

"nontcpzombie":<Integer_value>,

"reducedfintimeout":<Integer_value>,

"reducedrsttimeout":<Integer_value>,

"newconnidletimeout":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/nstimeout? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nstimeout":{

"zombie":true,

"client":true,

"server":true,

"httpclient":true,

"httpserver":true,

"tcpclient":true,

"tcpserver":true,

"anyclient":true,

"anyserver":true,

"anytcpclient":true,

"anytcpserver":true,

"halfclose":true,

"nontcpzombie":true,

"reducedfintimeout":true,

"reducedrsttimeout":true,

"newconnidletimeout":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/nstimeout **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nstimeout": [ {

"zombie":<Integer_value>,

"client":<Integer_value>,

"server":<Integer_value>,

"httpclient":<Integer_value>,

"httpserver":<Integer_value>,

"tcpclient":<Integer_value>,

"tcpserver":<Integer_value>,

"anyclient":<Integer_value>,
```

```
"anyserver":<Integer_value>,

"halfclose":<Integer_value>,

"anytcpclient":<Integer_value>,

"anytcpserver":<Integer_value>,

"nontcpzombie":<Integer_value>,

"reducedfintimeout":<Integer_value>,

"reducedrsttimeout":<Integer_value>,

"newconnidletimeout":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

nstimer

Configuration for Timer resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Timer name. Minimum length = 1
interval	<Integer>	Read-write	The frequency at which the policies bound to this timer are invoked. The minimum value is 20 msec. The maximum value is 20940 in

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			seconds and 349 in minutes. Default value: 5 Minimum value = 1 Maximum value = 20940000
unit	<String>	Read-write	Timer interval unit. Default value: SEC Possible values = SEC, MIN
comment	<String>	Read-write	Comments associated with this timer.
newname	<String>	Read-write	The new name of the timer. Minimum length = 1
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT
- RENAME

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/nstimer **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nstimer":{

<b>"name":<String_value>,

</b><b>"interval":<Integer_value>,
```

```
</b>"unit":<String_value>,

"comment":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/nstimer/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/nstimer **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nstimer":{

<b>"name":<String_value>,

</b>"interval":<Integer_value>,

"unit":<String_value>,
```

```
"comment":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/nstimer? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nstimer":{

<b>"name":<String_value>,

</b>"interval":true,

"unit":true,

"comment":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

RENAME

URL: http:// <netscaler-ip-address> /nitro/v1/config/nstimer? **action=rename HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nstimer":{

<b>"name":<String_value>,

</b><b>"newname":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/nstimer **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/nstimer? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/nstimer? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of nstimer resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/nstimer? **view=summary**

Use this query-parameter to get the summary output of nstimer resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/nstimer? **pagesize=#no;pageno=#no**

Use this query-parameter to get the nstimer resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nstimer": [ {

"name":<String_value>,

"interval":<Integer_value>,

"unit":<String_value>,

"comment":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/nstimer/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/nstimer/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/nstimer/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of nstimer resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "nstimer": [ {

"name":<String_value>,

"interval":<Integer_value>,

"unit":<String_value>,

"comment":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/nstimer? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nstimer": [ { "__count": "#no"} ] }
```

nstimer_autoscalepolicy_binding

Binding object showing the autoscalepolicy that can be bound to nstimer.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
gotopriorityexpression	<String>	Read-write	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
samplesize	<Integer>	Read-write	Denotes the sample size. Sample size value of 'x' means that previous '(x - 1)' policy's rule evaluation results and the current evaluation result are present with the binding. For

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			example, sample size of 10 means that there is a state of previous 9 policy evaluation results and also the current policy evaluation result. Default value: 3 Minimum value = 1 Maximum value = 32
policyname	<String>	Read-write	The timer policy associated with the timer.
vserver	<String>	Read-write	Name of the vserver which provides the context for the rule in timer policy. When not specified it is treated as a Global Default context.
threshold	<Integer>	Read-write	Denotes the threshold. If the rule of the policy in the binding relation evaluates 'threshold size' number of times in 'sample size' to true, then the corresponding action is taken. Its value needs to be less than or equal to the sample size value.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: 3 Minimum value = 1 Maximum value = 32
name	<String>	Read-write	Timer name. Minimum length = 1
priority	<Integer>	Read-write	Specifies the priority of the timer policy.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/nstimer_autoscalepolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"nstimer_autoscalepolicy_binding":{

<b>"name":<String_value>,

</b><b>"policyname":<String_value>,

</b><b>"priority":<Integer_value>,

</b>"gotopriorityexpression":<String_value>,

"vserver":<String_value>,

"samplesize":<Integer_value>,

"threshold":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/nstimer_autoscalepolicy_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ nstimer_autoscalepolicy_binding/ name_value<String> ? **args= policyname:<String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/nstimer_autoscalepolicy_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ nstimer_autoscalepolicy_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of nstimer_autoscalepolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/nstimer_autoscalepolicy_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the nstimer_autoscalepolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "nstimer_autoscalepolicy_binding": [ {

"gotopriorityexpression":<String_value>,

"samplesize":<Integer_value>,

"policyname":<String_value>,

"vserver":<String_value>,

"threshold":<Integer_value>,

"name":<String_value>,

"priority":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/nstimer_autoscalepolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/nstimer_autoscalepolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "nstimer_autoscalepolicy_binding": [ {

"gotopriorityexpression":<String_value>,

"samplesize":<Integer_value>,

"policyname":<String_value>,

"vserver":<String_value>,

"threshold":<Integer_value>,

"name":<String_value>,

"priority":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/nstimer_autoscalepolicy_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"nstimer_autoscalepolicy_binding": [ { "__count": "#no"} ] }
```

nstimer_binding

Binding object which returns the resources bound to nstimer.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Timer name. Minimum length = 1
nstimer_autoscalepolicy_binding	<nstimer_autoscalepolicy_binding[]>	Read-only	autoscalepolicy that can be bound to nstimer.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/nstimer_binding/ name_value<String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nstimer_binding": [ {

"name":<String_value>,

"nstimer_autoscalepolicy_binding":<nstimer_autoscalepolicy_binding[]_value
>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/nstimer_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/nstimer_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nstimer_binding": [ {

"name":<String_value>,

"nstimer_autoscalepolicy_binding":<nstimer_autoscalepolicy_binding[]_value
>
```

```
}]}
```

nstimezone

Configuration for 0 resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
value	<String>	Read-write	. Maximum length = 64
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.
- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of

creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/nstimezone **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/nstimezone? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/nstimezone? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of nstimezone resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/nstimezone? **view=summary**

Use this query-parameter to get the summary output of nstimezone resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/nstimezone? **pagesize=#no;pageno=#no**

Use this query-parameter to get the nstimezone resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nstimezone": [ {

"value":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/nstimezone/ value_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/nstimezone/ value_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/nstimezone/ value_value<String> ? **view=summary**

Use this query-parameter to get the summary output of nstimezone resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "nstimezone": [ {

"value":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/nstimezone? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nstimezone": [ { "__count": "#no"} ] }
```

nstrafficdomain

Configuration for Traffic Domain resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
td	<Integer>	Read-write	Integer value that uniquely identifies a traffic domain. Minimum value = 1 Maximum value = 4094
aliasname	<String>	Read-write	Name of traffic domain being added. Minimum length = 1 Maximum length = 31
vmac	<String>	Read-write	Associate the traffic domain with a VMAC address instead of with VLANs. The Citrix ADC then sends the VMAC address of the traffic domain in all responses to ARP queries for network entities in that domain. As a result, the ADC can segregate subsequent incoming traffic for this traffic domain on the basis of the destination MAC address,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			because the destination MAC address is the VMAC address of the traffic domain. After creating entities on a traffic domain, you can easily manage and monitor them by performing traffic domain level operations. Default value: DISABLED Possible values = ENABLED, DISABLED
state	<String>	Read-only	The state of TrafficDmain. Default value: ENABLED Possible values = ENABLED, DISABLED
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- CLEAR
- ENABLE

- DISABLE
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/nstrafficdomain **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nstrafficdomain":{

<b>"td":<Integer_value>,

</b>"aliasname":<String_value>,

"vmac":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/nstrafficdomain/ td_value<Integer> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

CLEAR

URL: http:// <netscaler-ip-address> /nitro/v1/config/nstrafficdomain? **action=clear HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nstrafficdomain":{

<b>"td":<Integer_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

ENABLE

URL: http:// <netscaler-ip-address> /nitro/v1/config/nstrafficdomain? **action=enable HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nstrafficdomain":{

<b>"td":<Integer_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DISABLE

URL: http:// <netscaler-ip-address> /nitro/v1/config/nstrafficdomain? **action=disable HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nstrafficdomain":{

<b>"td":<Integer_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/nstrafficdomain **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/nstrafficdomain? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/nstrafficdomain? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of nstrafficdomain resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/nstrafficdomain? **view=summary**

Use this query-parameter to get the summary output of nstrafficdomain resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/nstrafficdomain? **pagesize=#no;pageno=#no**

Use this query-parameter to get the nstrafficdomain resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nstrafficdomain": [ {

"td":<Integer_value>,

"aliasname":<String_value>,

"vmac":<String_value>,

"state":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/nstrafficdomain/ td_value<Integer> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/nstrafficdomain/ td_value<Integer> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/nstrafficdomain/ td_value<Integer> ? **view=summary**

Use this query-parameter to get the summary output of nstrafficdomain resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "nstrafficdomain": [ {

"td":<Integer_value>,

"aliasname":<String_value>,

"vmac":<String_value>,

"state":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/nstrafficdomain? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nstrafficdomain": [ { "__count": "#no"} ] }
```

nstrafficdomain_binding

Binding object which returns the resources bound to nstrafficdomain.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
td	<Integer>	Read-write	Integer value that uniquely identifies a traffic domain. Minimum value = 1 Maximum value = 4094
nstrafficdomain_vlan_binding	<nstrafficdomain_vlan_binding[]>	Read-only	vlan that can be bound to nstrafficdomain.
nstrafficdomain_bridgegroup_binding	<nstrafficdomain_bridgegroup_binding[]>	Read-only	bridgegroup that can be bound to nstrafficdomain.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
nstrafficdomain_vxlan_binding	<nstrafficdomain_vxlan_binding[]>	Read-only	vxlan that can be bound to nstrafficdomain.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/nstrafficdomain_binding/ td_value<Integer>
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nstrafficdomain_binding": [ {

"td":<Integer_value>,

"nstrafficdomain_vxlan_binding":<nstrafficdomain_vxlan_binding[]_value>,

"nstrafficdomain_bridgegroup_binding":<nstrafficdomain_bridgegroup_binding
[]_value>,

"nstrafficdomain_vlan_binding":<nstrafficdomain_vlan_binding[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/nstrafficdomain_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ nstrafficdomain_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nstrafficdomain_binding": [ {

"td":<Integer_value>,

"nstrafficdomain_vxlan_binding":<nstrafficdomain_vxlan_binding[]_value>,

"nstrafficdomain_bridgegroup_binding":<nstrafficdomain_bridgegroup_binding
[]_value>,

"nstrafficdomain_vlan_binding":<nstrafficdomain_vlan_binding[]_value>

}]}
```

nstrafficdomain_bridgegroup_binding

Binding object showing the bridgegroup that can be bound to nstrafficdomain.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
bridgegroup	<Integer>	Read-write	ID of the configured bridge to bind to this traffic domain. More

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			than one bridge group can be bound to a traffic domain, but the same bridge group cannot be a part of multiple traffic domains. Minimum value = 1 Maximum value = 1000
td	<Integer>	Read-write	Integer value that uniquely identifies a traffic domain. Minimum value = 1 Maximum value = 4094
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/nstrafficdomain_bridgegroup_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"nstrafficdomain_bridgegroup_binding":{

<b>"td":<Integer_value>,

</b>"bridgegroup":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/nstrafficdomain_bridgegroup_binding/ td_value<Integer> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ nstrafficdomain_bridgegroup_binding/ td_value<Integer> ? **args=bridgegroup: <Integer_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/nstrafficdomain_bridgegroup_binding/ td_value<Integer> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ nstrafficdomain_bridgegroup_binding/ td_value<Integer> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of nstrafficdomain_bridgegroup_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/nstrafficdomain_bridgegroup_binding/ td_value<Integer> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the nstrafficdomain_bridgegroup_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "nstrafficdomain_bridgegroup_binding": [ {

"bridgegroup":<Integer_value>,

"td":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/nstrafficdomain_bridgegroup_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/nstrafficdomain_bridgegroup_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "nstrafficdomain_bridgegroup_binding": [ {

"bridgegroup":<Integer_value>,

"td":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/nstrafficdomain_bridgegroup_binding/td_value<Integer> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"nstrafficdomain_bridgegroup_binding": [ { "__count": "#no"} ] }
```

nstrafficdomain_vlan_binding

Binding object showing the vlan that can be bound to nstrafficdomain.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
td	<Integer>	Read-write	Integer value that uniquely identifies a traffic domain. Minimum value = 1 Maximum value = 4094
vlan	<Integer>	Read-write	ID of the VLAN to bind to this traffic domain. More than one VLAN can be bound to a traffic domain, but the same VLAN cannot be a part of multiple traffic domains. Minimum value = 1 Maximum value = 4094
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/nstrafficdomain_vlan_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"nstrafficdomain_vlan_binding":{

<b>"td":<Integer_value>,

</b>"vlan":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/nstrafficdomain_vlan_binding/ td_value<Integer> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ nstrafficdomain_vlan_binding/ td_value<Integer> ? **args=vlan: <Integer_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/nstrafficdomain_vlan_binding/ td_value<Integer> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ nstrafficdomain_vlan_binding/ td_value<Integer> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of nstrafficdomain_vlan_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/nstrafficdomain_vlan_binding/ td_value<Integer> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the nstrafficdomain_vlan_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "nstrafficdomain_vlan_binding": [ {

"td":<Integer_value>,

"vlan":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/nstrafficdomain_vlan_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/nstrafficdomain_vlan_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "nstrafficdomain_vlan_binding": [ {

"td":<Integer_value>,

"vlan":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/nstrafficdomain_vlan_binding/ td_value<Integer> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"nstrafficdomain_vlan_binding": [ { "__count": "#no"} ] }
```

nstrafficdomain_vxlan_binding

Binding object showing the vxlan that can be bound to nstrafficdomain.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
vxlan	<Integer>	Read-write	ID of the VXLAN to bind to this traffic domain. More than one VXLAN can be bound to a traffic domain, but the same VXLAN cannot be a part of multiple traffic domains. Minimum value = 1 Maximum value = 16777215
td	<Integer>	Read-write	Integer value that uniquely identifies a traffic domain. Minimum value = 1 Maximum value = 4094
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/nstrafficdomain_vxlan_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"nstrafficdomain_vxlan_binding":{

<b>"td":<Integer_value>,

</b>"vxlan":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/nstrafficdomain_vxlan_binding/ td_value<Integer> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ nstrafficdomain_vxlan_binding/ td_value<Integer> ? **args=vxlan: <Integer_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/nstrafficdomain_vxlan_binding/ td_value<Integer> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ nstrafficdomain_vxlan_binding/ td_value<Integer> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of nstrafficdomain_vxlan_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/nstrafficdomain_vxlan_binding/ td_value<Integer> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the nstrafficdomain_vxlan_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "nstrafficdomain_vxlan_binding": [ {

"vxlan":<Integer_value>,

"td":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/nstrafficdomain_vxlan_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/nstrafficdomain_vxlan_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "nstrafficdomain_vxlan_binding": [ {

"vxlan":<Integer_value>,

"td":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/nstrafficdomain_vxlan_binding/ td_value<Integer> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"nstrafficdomain_vxlan_binding": [ { "__count": "#no"} ] }
```

nsvariable

Configuration for variable resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Variable name. This follows the same syntax rules as other expression entity names: It must begin with an alpha character (A-Z or a-z) or an underscore (_). The rest of the characters must be alpha, numeric (0-9) or underscores. It cannot be re or xp (reserved for regular and XPath expressions). It cannot be an expression reserved word (e.g. SYS or HTTP). It cannot be used for an existing expression object (HTTP callout, patset, dataset, stringmap, or named expression). Minimum length = 1
type	<String>	Read-write	Specification of the variable type; one of the following:

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			ulong - singleton variable with an unsigned 64-bit value. text(value-max-size) - singleton variable with a text string value. map(text(key-max-size),ulong,max-entries) - map of text string keys to unsigned 64-bit values. map(text(key-max-size),text(value-max-size),max-entries) - map of text string keys to text string values. where value-max-size is a positive integer that is the maximum number of bytes in a text string value. key-max-size is a positive integer that is the maximum number of bytes in a text string key.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			max-entries is a positive integer that is the maximum number of entries in a map variable. For a global singleton text variable, value-max-size <= 64000. For a global map with ulong values, key-max-size <= 64000. For a global map with text values, key-max-size + value-max-size <= 64000. max-entries is a positive integer that is the maximum number of entries in a map variable. This has a theoretical maximum of 2\^64-1, but in actual use will be much smaller, considering the memory available for use by the map. Example:

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			map(text(10),text(20),100) specifies a map of text string keys (max size 10 bytes) to text string values (max size 20 bytes), with 100 max entries. Minimum length = 1
scope	<String>	Read-write	Scope of the variable: global - (default) one set of values visible across all Packet Engines on a standalone Citrix ADC, an HA pair, or all nodes of a cluster transaction - one value for each request-response transaction (singleton variables only; no expiration). Default value: global Possible values = global, transaction
iffull	<String>	Read-write	Action to perform if an assignment to a map exceeds its

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			configured max-entries: lru - (default) reuse the least recently used entry in the map. undef - force the assignment to return an undefined (Undef) result to the policy executing the assignment. Default value: lru Possible values = undef, lru
ifvaluetoobig	<String>	Read-write	Action to perform if an value is assigned to a text variable that exceeds its configured max-size, or if a key is used that exceeds its configured max-size: truncate - (default) truncate the text string to the first max-size bytes and proceed. undef - force the assignment or expression evaluation to return

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			an undefined (Undef) result to the policy executing the assignment or expression. Default value: truncate Possible values = undef, truncate
ifnovalue	<String>	Read-write	Action to perform if on a variable reference in an expression if the variable is single-valued and uninitialized or if the variable is a map and there is no value for the specified key: init - (default) initialize the single-value variable, or create a map entry for the key and the initial value, using the -init value or its default. undef - force the expression evaluation to return an undefined (Undef) result to the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			policy executing the expression. Default value: init Possible values = undef, init
init	<String>	Read-write	Initialization value for this variable, to which a singleton variable or map entry will be set if it is referenced before an assignment action has assigned it a value. If the singleton variable or map entry already has been assigned a value, setting this parameter will have no effect on that variable value. Default: 0 for ulong, NULL for text.
expires	<Integer>	Read-write	Value expiration in seconds. If the value is not referenced within the expiration period it will be deleted. 0 (the default) means no expiration. Minimum value = 0 Maximum value = 31622400

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
comment	<String>	Read-write	Comments associated with this variable.
referencecount	<Integer>	Read-only	The number of references to the variable in expressions and assignments.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- UPDATE
- UNSET
- DELETE
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of

creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsvariable **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nsvariable":{

<b>"name":<String_value>,

</b><b>"type":<String_value>,

</b>"scope":<String_value>,

"iffull":<String_value>,

"ifvaluetoobig":<String_value>,

"ifnovalue":<String_value>,

"init":<String_value>,

"expires":<Integer_value>,
```

```
"comment":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsvariable **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nsvariable":{

<b>"name":<String_value>,

</b>"type":<String_value>,

"iffull":<String_value>,

"ifvaluetoobig":<String_value>,

"ifnovalue":<String_value>,

"init":<String_value>,

"expires":<Integer_value>,

"comment":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsvariable? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nsvariable":{

<b>"name":<String_value>,

</b>"iffull":true,

"ifvaluetoobig":true,

"ifnovalue":true,

"init":true,

"expires":true,

"comment":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsvariable/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsvariable **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/nsvariable? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/nsvariable? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of nsvariable resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/nsvariable? **view=summary**

Use this query-parameter to get the summary output of nsvariable resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/nsvariable? **pagesize=#no;pageno=#no**

Use this query-parameter to get the nsvariable resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nsvariable": [ {

"name":<String_value>,

"type":<String_value>,

"scope":<String_value>,

"iffull":<String_value>,

"ifvaluetoobig":<String_value>,

"ifnovalue":<String_value>,

"init":<String_value>,

"expires":<Integer_value>,

"comment":<String_value>,

"referencecount":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsvariable/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/nsvariable/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/nsvariable/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of nsvariable resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "nsvariable": [ {

"name":<String_value>,

"type":<String_value>,

"scope":<String_value>,

"iffull":<String_value>,

"ifvaluetoobig":<String_value>,

"ifnovalue":<String_value>,

"init":<String_value>,

"expires":<Integer_value>,
```

```
"comment":<String_value>,

"referencecount":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsvariable? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nsvariable": [ { "__count": "#no"} ] }
```

nsvariablevalues

Configuration for Variable runtime data information resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
nodeid	<Integer>	Read-write	Unique number that identifies the cluster node. Minimum value = 0 Maximum value = 31
variablekey	<String>	Read-only	.
variablevalue	<String>	Read-only	.
variabledata	<String>	Read-only	.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of

creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsvariablevalues **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/nsvariablevalues? **args= name:<String_value>, nodeid: <Integer_value>**

Use this query-parameter to get nsvariablevalues resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/config/nsvariablevalues? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/nsvariablevalues? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of nsvariablevalues resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/nsvariablevalues? **view=summary**

Use this query-parameter to get the summary output of nsvariablevalues resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/nsvariablevalues? **pagesize=#no;pageno=#no**

Use this query-parameter to get the nsvariablevalues resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nsvariablevalues": [ {

<b>name:<String_value>,</
b>nodeid:<Integer_value>"variablekey":<String_value>,

"variablevalue":<String_value>,

"variabledata":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsvariablevalues/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/nsvariablevalues/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/nsvariablevalues/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of nsvariablevalues resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "nsvariablevalues": [ {

<b>name:<String_value>,</
b>nodeid:<Integer_value>"variablekey":<String_value>,

"variablevalue":<String_value>,

"variabledata":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsvariablevalues? **args= name:<String_value>, nodeid: <Integer_value> ;count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nsvariablevalues": [ { "__count": "#no"} ] }
```

nsversion

Configuration for version resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
installedversion	<Boolean>	Read-write	Installed version.
version	<String>	Read-only	Version.
mode	<Integer>	Read-only	Kernel mode (KMPE/VMPE).
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsversion

Query-parameters:

args

http:// <netscaler-ip-address> /nitro/v1/config/nsversion? **args=installedversion: <Boolean_value>**

Use this query-parameter to get nsversion resources based on additional properties.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nsversion": [ {

installedversion:<Boolean_value>"version":<String_value>,

"mode":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

nsvpxparam

Configuration for "VPX" resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
masterclockcpu1	<String>	Read-write	This argument is deprecated. Possible values = YES, NO

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
cpuyield	<String>	Read-write	This setting applicable in virtual appliances, is to affect the cpu yield(relinquishing the cpu resources) in any hypervised environment. * There are 3 options for the behavior: 1. YES - Allow the Virtual Appliance to yield its vCPUs periodically, if there is no data traffic. 2. NO - Virtual Appliance will not yield the vCPU. 3. DEFAULT - Restores the default behaviour, according to the license. * Its behavior in different scenarios: 1. As this setting is node specific only, it will not be propagated to other nodes, when executed on

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Cluster(CLIP) and HA(Primary). 2. In cluster setup, use '-ownerNode' to specify ID of the cluster node. 3. This setting is a system wide implementation and not granular to vCPUs. 4. No effect on the management PE. Default value: DEFAULT Possible values = DEFAULT, YES, NO
ownernode	<Integer>	Read-write	ID of the cluster node for which you are setting the cpuyield and/or KVMVirtioMultiqueue . It can be configured only through the cluster IP address. Default value: 255 Minimum value = 0 Maximum value = 31
kvmvirtiomultiqueue	<String>	Read-write	This setting applicable on KVM VPX with virtio NICs,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			is to configure multiple queues for all virtio interfaces. * There are 2 options for this behavior: 1. YES - Allows VPX to use multiple queues for each virtio interface as configured through the KVM Hypervisor. 2. NO - Each virtio interface within VPX will use a single queue for transmit and receive. * Its behavior in different scenarios: 1. As this setting is node specific only, it will not be propagated to other nodes, when executed on Cluster(CLIP) and HA(Primary). 2. In cluster setup, use '-ownerNode' to specify ID of the cluster node.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: NO Possible values = YES, NO
vpxenvironment	<String>	Read-only	Shows VPX Running Environmentrunning 0 VPX ON PREM, 1 AWS, 2 OPENSTACK 3 Azure, 4 GCP CLoud . Possible values = VPX, AWSCLOUD, OPENSTACKCLOUD, AZURECLOUD, GOOGLECLOUD, ALICLOUD, IBMCLOUD
memorystatus	<String>	Read-only	Provides the information about memory status. Possible values = Sufficent, Insufficent
cloudproductcode	<String>	Read-only	Cloud Product Code Description . Maximum length = 127
vpxoemcode	<Integer>	Read-only	OEM Distribution Code. .
technicalsupportpin	<String>	Read-only	Technical Support PIN for cloud subscription VMs. Maximum length = 15

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- UPDATE
- UNSET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsvpxparam **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nsvpxparam":{

"masterclockcpu1":<String_value>,

"cpuyield":<String_value>,

"ownernode":<Integer_value>,

"kvmvirtiomultiqueue":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsvpxparam? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nsvpxparam":{

"masterclockcpu1":true,

"cpuyield":true,

"ownernode":<Integer_value>,

"kvmvirtiomultiqueue":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsvpxparam **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/nsvpxparam? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/nsvpxparam? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of nsvpxparam resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/nsvpxparam? **view=summary**

Use this query-parameter to get the summary output of nsvpxparam resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/nsvpxparam? **pagesize=#no;pageno=#no**

Use this query-parameter to get the nsvpxparam resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nsvpxparam": [ {

"cpuyield":<String_value>,

"ownernode":<Integer_value>,

"masterclockcpu1":<String_value>,

"vpxenvironment":<String_value>,

"memorystatus":<String_value>,

"cloudproductcode":<String_value>,

"vpxoemcode":<Integer_value>,

"technicalsupportpin":<String_value>,

"kvmvirtiomultiqueue":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsvpxparam? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nsvpxparam": [ { "__count": "#no"} ] }
```

nsweblogparam

Configuration for Web log parameters resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
buffersizemb	<Integer>	Read-write	Buffer size, in MB, allocated for log transaction data on the system. The maximum value is limited to the memory available on the system. Default value: 16

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum value = 1 Maximum value = 4294967294LU
customreqhdrs	<String[]>	Read-write	Name(s) of HTTP request headers whose values should be exported by the Web Logging feature. Minimum length = 1
customrsphdrs	<String[]>	Read-write	Name(s) of HTTP response headers whose values should be exported by the Web Logging feature. Minimum length = 1
builtin	<String[]>	Read-only	Flag to determine if log bufs is built-in or not. Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL
feature	<String>	Read-only	The feature to be checked while applying this config.
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- UPDATE

- UNSET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsweblogparam **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nsweblogparam":{

"buffersizemb":<Integer_value>,

"customreqhdrs":<String[]_value>,

"customrsphdrs":<String[]_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsweblogparam? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nsweblogparam":{

"buffersizemb":true,

"customreqhdrs":true,

"customrsphdrs":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsweblogparam **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nsweblogparam": [ {

"buffersizemb":<Integer_value>,

"customreqhdrs":<String[]_value>,

"customrsphdrs":<String[]_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

nsxmlnamespace

Configuration for XML namespace resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
prefix	<String>	Read-write	XML prefix. Minimum length = 1
Namespace	<String>	Read-write	Expanded namespace for which the XML prefix is provided. Minimum length = 1
description	<String>	Read-write	Description for the prefix. Minimum length = 1
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsxmlnamespace **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nsxmlnamespace":{

<b>"prefix":<String_value>,

</b><b>"Namespace":<String_value>,

</b>"description":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsxmlnamespace/ prefix_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsxmlnamespace **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nsxmlnamespace":{

<b>"prefix":<String_value>,

</b>"Namespace":<String_value>,

"description":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsxmlnamespace? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"nsxmlnamespace":{

<b>"prefix":<String_value>,

</b>"Namespace":true,

"description":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsxmlnamespace **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/nsxmlnamespace? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/nsxmlnamespace? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of nsxmlnamespace resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/nsxmlnamespace? **view=summary**

Use this query-parameter to get the summary output of nsxmlnamespace resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/nsxmlnamespace? **pagesize=#no;pageno=#no**

Use this query-parameter to get the nsxmlnamespace resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nsxmlnamespace": [ {

"prefix":<String_value>,

"Namespace":<String_value>,

"description":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsxmlnamespace/ prefix_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/nsxmlnamespace/ prefix_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/nsxmlnamespace/ prefix_value<String> ? **view=summary**

Use this query-parameter to get the summary output of nsxmlnamespace resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "nsxmlnamespace": [ {

"prefix":<String_value>,

"Namespace":<String_value>,

"description":<String_value>,

"_nextgenapiresource":<String_value>
```

```
}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/nsxmlnamespace? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "nsxmlnamespace": [ { "__count": "#no"} ] }
```

reboot

Configuration for 0 resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
warm	<Boolean>	Read-write	Restarts the Citrix ADC software without rebooting the underlying operating system. The session terminates and you

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			must log on to the appliance after it has restarted. Note: This argument is required only for nCore appliances. Classic appliances ignore this argument.

Operations

(click to see Properties)

- REBOOT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

REBOOT

URL: http:// <netscaler-ip-address> /nitro/v1/config/reboot **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"reboot":{

"warm":<Boolean_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

shutdown

Configuration for 0 resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION

Operations

(click to see Properties)

- SHUTDOWN

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

SHUTDOWN

URL: http:// <netscaler-ip-address> /nitro/v1/config/shutdown

HTTP Method: POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"shutdown":{

}}
```

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

ntp

NTP

NTP configuration.

NAME	DESCRIPTION
ntpparam	Configuration for NTP parameter
ntpserver	Configuration for NTP server
ntpstatus	Configuration for ntp status
ntpsync	Configuration for NTP sync

ntpparam

Configuration for NTP parameter resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
authentication	<String>	Read-write	Apply NTP authentication, which enables the NTP client (Citrix ADC) to verify that the server

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			is in fact known and trusted. Default value: YES Possible values = YES, NO
trustedkey	<Integer[]>	Read-write	Key identifiers that are trusted for server authentication with symmetric key cryptography in the keys file. Minimum value = 1 Maximum value = 65534
autokeylogsec	<Integer>	Read-write	Autokey protocol requires the keys to be refreshed periodically. This parameter specifies the interval between regenerations of new session keys. In seconds, expressed as a power of 2. Default value: 12 Minimum value = 0 Maximum value = 32
revokelogsec	<Integer>	Read-write	Interval between re-randomizations of the autokey seeds to prevent brute-force attacks on the autokey algorithms.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: 16 Minimum value = 0 Maximum value = 32
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- UPDATE
- UNSET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/ntpparam **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"ntpparam":{

"authentication":<String_value>,

"trustedkey":<Integer[]_value>,

"autokeylogsec":<Integer_value>,

"revokelogsec":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/ntpparam? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"ntpparam":{

"authentication":true,

"trustedkey":true,

"autokeylogsec":true,

"revokelogsec":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/ntpparam **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "ntpparam": [ {

"authentication":<String_value>,

"trustedkey":<Integer[]_value>,
```

```
"autokeylogsec":<Integer_value>,

"revokelogsec":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

ntpserver

Configuration for NTP server resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
serverip	<String>	Read-write	IP address of the NTP server. Minimum length = 1
servername	<String>	Read-write	Fully qualified domain name of the NTP server.
minpoll	<Integer>	Read-write	Minimum time after which the NTP server must poll the NTP messages. In seconds, expressed as a power of 2. Minimum value = 4 Maximum value = 17
maxpoll	<Integer>	Read-write	Maximum time after which the NTP server must poll the NTP messages. In

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			seconds, expressed as a power of 2. Minimum value = 4 Maximum value = 17
autokey	<Boolean>	Read-write	Use the Autokey protocol for key management for this server, with the cryptographic values (for example, symmetric key, host and public certificate files, and sign key) generated by the ntp-keygen utility. To require authentication for communication with the server, you must set either the value of this parameter or the key parameter.
key	<Integer>	Read-write	Key to use for encrypting authentication fields. All packets sent to and received from the server must include authentication fields encrypted by using this key. To require authentication for communication with the server, you must set either the value of this parameter or

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			the autokey parameter. Minimum value = 1 Maximum value = 65534
preferredntpserver	<String>	Read-write	Preferred NTP server. The Citrix ADC chooses this NTP server for time synchronization among a set of correctly operating hosts. Default value: NO Possible values = YES, NO
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/ntpserver **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"ntpserver":{

"serverip":<String_value>,

"servername":<String_value>,

"minpoll":<Integer_value>,

"maxpoll":<Integer_value>,

"autokey":<Boolean_value>,
```

```
"key":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/ntpserver/ serverip_value<String> **Query-parameters: args=servername: <String_value>**

update

URL: http:// <netscaler-ip-address> /nitro/v1/config/ntpserver **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"ntpserver":{

"serverip":<String_value>,

"servername":<String_value>,

"minpoll":<Integer_value>,

"maxpoll":<Integer_value>,

"preferredntpserver":<String_value>,

"autokey":<Boolean_value>,

"key":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

unset

URL: http:// <netscaler-ip-address> /nitro/v1/config/ntpserver? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"ntpserver":{

"serverip":<String_value>,

"servername":<String_value>,

"autokey":true,

"minpoll":true,

"maxpoll":true,

"preferredntpserver":true,

"key":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

get (all)

URL: http:// <netscaler-ip-address> /nitro/v1/config/ntpserver **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/ntpserver? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/ntpserver? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of ntpserver resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/ntpserver? **view=summary**

Use this query-parameter to get the summary output of ntpserver resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/ntpserver? **pagesize=#no;pageno=#no**

Use this query-parameter to get the ntpserver resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "ntpserver": [ {

"serverip":<String_value>,
```

```
"servername":<String_value>,

"minpoll":<Integer_value>,

"maxpoll":<Integer_value>,

"preferredntpserver":<String_value>,

"autokey":<Boolean_value>,

"key":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

count

URL: http:// <netscaler-ip-address> /nitro/v1/config/ntpserver? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "ntpserver": [ { "__count": "#no"} ] }
```

ntpstatus

Configuration for ntp status resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
response	<String>	Read-write	.
_nextgenapiresource	<String>	Read-write	.

Operations

(click to see Properties)

- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/ntpstatus

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "ntpstatus": [ {

"response":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

ntpsync

Configuration for NTP sync resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
state	<String>	Read-write	Show NTP status. Possible values = ENABLED, DISABLED
_nextgenapiresource	<String>	Read-write	.

Operations

(click to see Properties)

- ENABLE
- DISABLE
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ENABLE

URL: http:// <netscaler-ip-address> /nitro/v1/config/ntpsync? **action=enable HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"ntpsync":{

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DISABLE

URL: http:// <netscaler-ip-address> /nitro/v1/config/ntpsync? **action=disable HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"ntpsync":{

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/ntpsync **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "ntpsync": [ {

"state":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

pcp

Pcp

Port Control Protocol Configuration.

NAME	DESCRIPTION
pcpmap	Configuration for server

NAME	DESCRIPTION
pcpprofile	Configuration for PCP Profile
pcpserver	Configuration for server

pcpmap

Configuration for server resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
nattype	<String>	Read-write	Type of sessions to be displayed. Default value: NAT44 Possible values = NAT44, DS-Lite, NAT64
pcpsrcip	<String>	Read-only	Internal IP address.
subscrip	<String>	Read-only	IPV4 src address of Client in DS-Lite.
pcpsrcport	<Integer>	Read-only	Internal Port. Range 1 - 65535 * in CLI is represented as 65535 in NITRO API
pcpdstip	<String>	Read-only	Remote PEER IP address.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
pcpdstport	<Integer>	Read-only	Remote PEER Port. Range 1 - 65535 * in CLI is represented as 65535 in NITRO API
pcpnatip	<String>	Read-only	External IP address.
pcpnatport	<Integer>	Read-only	External Port Number. Range 1 - 65535 * in CLI is represented as 65535 in NITRO API
pcpprotocol	<String>	Read-only	Protocol of the PCP mapping. Possible values = HopOpt, icmp, igmp, ggp, ipv4, st, tcp, udp
pcpaddr	<Integer>	Read-only	Address of PCP Map entity.
pcpnounce	<Integer>	Read-only	PCP Mapping Nounce.
pcprefcnt	<Integer>	Read-only	Refcount, which indicates how many session is active.
pcplifetime	<Integer>	Read-only	Integer value that shows the requested lifetime.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/pcpmap **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/pcpmap? **args=nattype: <String_value>**

Use this query-parameter to get pcpmap resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/config/pcpmap? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/pcpmap? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of pcpmap resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/pcpmap? **view=summary**

Use this query-parameter to get the summary output of pcpmap resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/pcpmap? **pagesize=#no;pageno=#no**

Use this query-parameter to get the pcpmap resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "pcpmap": [ {

nattype:<String_value>"pcpsrcip":<String_value>,

"subscrip":<String_value>,

"pcpsrcport":<Integer_value>,

"pcpdstip":<String_value>,

"pcpdstport":<Integer_value>,

"pcpnatip":<String_value>,

"pcpnatport":<Integer_value>,

"pcpprotocol":<String_value>,

"pcpaddr":<Integer_value>,

"pcpnounce":<Integer_value>,

"pcprefcnt":<Integer_value>,

"pcplifetime":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/pcpmap? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "pcpmap": [ { "__count": "#no"} ] }
```

pcpprofile

Configuration for PCP Profile resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the PCP Profile. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my pcpProfile" or my pcpProfile).
mapping	<String>	Read-write	This argument is for enabling/disabling

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			the MAP opcode of current PCP Profile. Default value: ENABLED Possible values = ENABLED, DISABLED
peer	<String>	Read-write	This argument is for enabling/disabling the PEER opcode of current PCP Profile. Default value: ENABLED Possible values = ENABLED, DISABLED
minmaplife	<Integer>	Read-write	Integer value that identify the minimum mapping lifetime (in seconds) for a pcp profile. default(120s). Minimum value = 1 Maximum value = 2147483647
maxmaplife	<Integer>	Read-write	Integer value that identify the maximum mapping lifetime (in seconds) for a pcp profile. default(86400s = 24Hours). Minimum value = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum value = 2147483647
announcemulticount	<Integer>	Read-write	Integer value that identify the number announce message to be send. Default value: 10 Minimum value = 0 Maximum value = 65535
thirdparty	<String>	Read-write	This argument is for enabling/disabling the THIRD PARTY opcode of current PCP Profile. Default value: DISABLED Possible values = ENABLED, DISABLED
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)

- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/pcpprofile **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"pcpprofile":{

<b>"name":<String_value>,

</b>"mapping":<String_value>,

"peer":<String_value>,

"minmaplife":<Integer_value>,

"maxmaplife":<Integer_value>,

"announcemulticount":<Integer_value>,

"thirdparty":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/pcpprofile/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/pcpprofile **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"pcpprofile":{

<b>"name":<String_value>,

</b>"mapping":<String_value>,

"peer":<String_value>,

"minmaplife":<Integer_value>,

"maxmaplife":<Integer_value>,

"announcemulticount":<Integer_value>,

"thirdparty":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/pcpprofile? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"pcpprofile":{

<b>"name":<String_value>,
```

```
</b>"mapping":true,

"peer":true,

"minmaplife":true,

"maxmaplife":true,

"announcemulticount":true,

"thirdparty":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/pcpprofile **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/pcpprofile? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/pcpprofile? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of pcpprofile resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/pcpprofile? **view=summary**

Use this query-parameter to get the summary output of pcpprofile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/pcpprofile? **pagesize=#no;pageno=#no**

Use this query-parameter to get the pcpprofile resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "pcpprofile": [ {

"name":<String_value>,

"mapping":<String_value>,

"peer":<String_value>,

"minmaplife":<Integer_value>,

"maxmaplife":<Integer_value>,

"announcemulticount":<Integer_value>,

"thirdparty":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/pcpprofile/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/pcpprofile/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/pcpprofile/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of pcpprofile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "pcpprofile": [ {

"name":<String_value>,

"mapping":<String_value>,

"peer":<String_value>,

"minmaplife":<Integer_value>,
```

```
"maxmaplife":<Integer_value>,

"announcemulticount":<Integer_value>,

"thirdparty":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/pcpprofile? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "pcpprofile": [ { "__count": "#no"} ] }
```

pcpserver

Configuration for server resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the PCP server. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my pcpServer" or my pcpServer).
ipaddress	<String>	Read-write	The IP address of the PCP server.
port	<Integer>	Read-write	Port number for the PCP server. Default value: 5351 Range 1 - 65535 * in CLI is represented as 65535 in NITRO API
pcpprofile	<String>	Read-write	pcp profile name.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/pcpserver **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"pcpserver":{

<b>"name":<String_value>,

</b><b>"ipaddress":<String_value>,

</b>"port":<Integer_value>,

"pcpprofile":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/pcpserver/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/pcpserver **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"pcpserver":{

<b>"name":<String_value>,

</b>"port":<Integer_value>,

"pcpprofile":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/pcpserver? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"pcpserver":{

<b>"name":<String_value>,

</b>"port":true,

"pcpprofile":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/pcpserver **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/pcpserver? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/pcpserver? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of pcpserver resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/pcpserver? **view=summary**

Use this query-parameter to get the summary output of pcpserver resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/pcpserver? **pagesize=#no;pageno=#no**

Use this query-parameter to get the pcpserver resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "pcpserver": [ {

"name":<String_value>,

"ipaddress":<String_value>,

"port":<Integer_value>,

"pcpprofile":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/pcpserver/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/pcpserver/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/pcpserver/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of pcpserver resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "pcpserver": [ {

"name":<String_value>,

"ipaddress":<String_value>,

"port":<Integer_value>,

"pcpprofile":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/pcpserver? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "pcpserver": [ { "__count": "#no"} ] }
```

policy

Policy

Policy configuration.

NAME	DESCRIPTION
policydataset	Configuration for TYPE set
policydataset_binding	Binding object showing the resources that can be bound to policydataset
policydataset_value_binding	Binding object showing the value that can be bound to policydataset
policyevaluation	Configuration for expr evaluation
policyexpression	Configuration for expression
policyhttpcallout	Configuration for HTTP callout
policymap	Configuration for map policy
policyparam	Configuration for policy parameter
policypatset	Configuration for PAT set
policypatset_binding	Binding object showing the resources that can be bound to policypatset
policypatset_pattern_binding	Binding object showing the pattern that can be bound to policypatset
policypatsetfile	Configuration for patset file
policystringmap	Configuration for string map

NAME	DESCRIPTION
policystringmap_binding	Binding object showing the resources that can be bound to policystringmap
policystringmap_pattern_binding	Binding object showing the pattern that can be bound to policystringmap
policytracing	
policyurlset	Configuration for URL set

policydataset

Configuration for TYPE set resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the dataset. Must not exceed 127 characters. Minimum length = 1
type	<String>	Read-write	Type of value to bind to the dataset. Possible values = ipv4, number, ipv6, ulong, double, mac
comment	<String>	Read-write	Any comments to preserve information about this dataset or a data bound to this dataset.
patsetfile	<String>	Read-write	File which contains list of patterns that needs to be bound to the dataset. A

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			patsetfile cannot be associated with multiple datasets.
dynamic	<String>	Read-write	This is used to populate internal dataset information so that the dataset can also be used dynamically in an expression. Here dynamically means the dataset name can also be derived using an expression. For example for a given dataset name "allow_test" it can be used dynamically as client.ip.src.equals_any("allow_" + http.req.url.path.get(1)). This cannot be used with default datasets. Default value: NO Possible values = YES, NO
dynamiconly	<Boolean>	Read-write	Shows only dynamic datasets when set true. Default value: 0
builtin	<String[]>	Read-only	Indicates that a variable is a built-in (SYSTEM INTERNAL) type.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL
feature	<String>	Read-only	The feature to be checked while applying this config.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of

creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/policydataset **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"policydataset":{

<b>"name":<String_value>,

</b><b>"type":<String_value>,

</b>"comment":<String_value>,

"patsetfile":<String_value>,

"dynamic":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/policydataset/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/policydataset **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"policydataset":{

<b>"name":<String_value>,

</b>"dynamic":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/policydataset? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"policydataset":{

<b>"name":<String_value>,

</b>"dynamic":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/policydataset **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/policydataset? **args=name: <String_value> ,dynamiconly: <Boolean_value>**

Use this query-parameter to get policydataset resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/config/policydataset? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/policydataset? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of policydataset resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/policydataset? **view=summary**

Use this query-parameter to get the summary output of policydataset resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/policydataset? **pagesize=#no;pageno=#no**

Use this query-parameter to get the policydataset resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "policydataset": [ {

name:<String_value>,dynamiconly:<Boolean_value>"type":<String_value>,

"comment":<String_value>,

"patsetfile":<String_value>,

"dynamic":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,
```

```
"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/policydataset/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/policydataset/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/policydataset/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of policydataset resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "policydataset": [ {

name:<String_value>,dynamiconly:<Boolean_value>"type":<String_value>,
```

```
"comment":<String_value>,

"patsetfile":<String_value>,

"dynamic":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/policydataset? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "policydataset": [ { "__count": "#no"} ] }
```

policydataset_binding

Binding object which returns the resources bound to policydataset.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the dataset. Must not exceed 127 characters. Minimum length = 1
policydataset_value_binding	<policydataset_value_binding[]>	Read-only	value that can be bound to policydataset.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/policydataset_binding/ name_value<String>
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "policydataset_binding": [ {

"name":<String_value>,

"policydataset_value_binding":<policydataset_value_binding[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/policydataset_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/policydataset_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "policydataset_binding": [ {

"name":<String_value>,

"policydataset_value_binding":<policydataset_value_binding[]_value>

}]}
```

policydataset_value_binding

Binding object showing the value that can be bound to policydataset.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
index	<Integer>	Read-write	The index of the value (ipv4, ipv6, number) associated with the set.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the dataset to which to bind the value. Minimum length = 1
value	<String>	Read-write	Value of the specified type that is associated with the dataset. For ipv4 and ipv6, value can be a subnet using the slash notation address/n, where address is the beginning of the subnet and n is the number of left-most bits set in the subnet mask, defining the end of the subnet. The start address will be masked by the subnet mask if necessary, for example for 192.128.128.0/10, the start address will be 192.128.0.0.
endrange	<String>	Read-write	The dataset entry is a range from <value> through <end_range>, inclusive. endRange cannot be used if value is an ipv4 or ipv6 subnet and endRange cannot itself be a subnet.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
comment	<String>	Read-write	Any comments to preserve information about this dataset or a data bound to this dataset.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/policydataset_value_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"policydataset_value_binding":{

<b>"name":<String_value>,

</b><b>"value":<String_value>,

</b>"index":<Integer_value>,

"endrange":<String_value>,

"comment":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/policydataset_value_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/

policydataset_value_binding/ name_value<String> ? **args= value:<String_value>, endrange: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/policydataset_value_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ policydataset_value_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of policydataset_value_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/policydataset_value_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the policydataset_value_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "policydataset_value_binding": [ {

"index":<Integer_value>,

"name":<String_value>,

"value":<String_value>,

"endrange":<String_value>,

"comment":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/policydataset_value_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/policydataset_value_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "policydataset_value_binding": [ {

"index":<Integer_value>,

"name":<String_value>,

"value":<String_value>,

"endrange":<String_value>,

"comment":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/policydataset_value_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"policydataset_value_binding": [ { "__count": "#no"} ] }
```

policyevaluation

Configuration for expr evaluation resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
expression	<String>	Read-write	Expression string. For example: http.req.body(100).contains("this").
action	<String>	Read-write	Rewrite action name. Supported rewrite action types are: -delete -delete_all -delete_http_header -insert_after -insert_after_all -insert_before -insert_before_all -insert_http_header -replace -replace_all . Minimum length = 1
type	<String>	Read-write	Indicates request or response input packet. Possible values = HTTP_REQ, HTTP_RES, TEXT

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
input	<String>	Read-write	Text representation of input packet.
pitmodifiedinputdata	<String>	Read-only	Text representation of packet after evaluating expression or rewrite action.
pitboolresult	<Boolean>	Read-only	Result of the expression in bool format.
pitnumresult	<Integer>	Read-only	Result of the expression in num format.
pitdoubleresult	<Double>	Read-only	Result of the expression in double format.
pitulongresult	<Integer>	Read-only	Result of the expression in unsigned long format.
pitrefresult	<String>	Read-only	Result of the expression in string format.
pitoffsetresult	<Integer>	Read-only	Offset of the resultant sting.
pitoffsetresultlen	<Integer>	Read-only	Offset length of the resultant sting.
istruncatedrefresult	<Boolean>	Read-only	Identify whether ref result is truncated result.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
pitboolevaltime	<Integer>	Read-only	Average evaluation time of bool type expression in nanoseconds.
pitnumevaltime	<Integer>	Read-only	Average evaluation time of num type expression in nanoseconds.
pitdoubleevaltime	<Integer>	Read-only	Average evaluation time of double type expression in nanoseconds.
pitulongevaltime	<Integer>	Read-only	Average evaluation time of unsigned long type expression in nanoseconds.
pitrefevaltime	<Integer>	Read-only	Average evaluation time of string type expression in nanoseconds.
pitoffsetevaltime	<Integer>	Read-only	Average evaluation time in finding offset of the resultant string in the input. Time is in nanoseconds.
pitactionevaltime	<Integer>	Read-only	Average evaluation time of rewrite action in nanoseconds.
pitoperationperformerarray	<String[]>	Read-only	Details of the operation Citrix ADC performed at various offsets during applying of rewrite action on input data.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Operation can be insertion, modfication or deletion. Possible values = INSERT, MODIFY, DELETE
pitoldoffsetarray	<Integer[]>	Read-only	Details of the offsets in the input data at which Citrix ADC either inserted or modified or deleted data during applying of rewrite action.
pitnewoffsetarray	<Integer[]>	Read-only	Details of the offsets in the output data at which Citrix ADC either inserted or modified or deleted data during applying of rewrite action.
pitoffsetlengtharray	<Integer[]>	Read-only	Details of the lengths of the data which Citrix ADC modified or deleted during applying of rewrite action.
pitoffsetnewlengtharray	<Integer[]>	Read-only	Details of the lengths of the data which Citrix ADC either inserted or modified during applying of rewrite action.
pitboolerrorresult	<String>	Read-only	Result of the bool type expression if any error occurs during evaluation.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Result will be in string format.
pitnumerrorresult	<String>	Read-only	Result of the num type expression if any error occurs during evaluation. Result will be in string format.
pitdoubleerrorresult	<String>	Read-only	Result of the double type expression if any error occurs during evaluation. Result will be in string format.
pitulongerrorresult	<String>	Read-only	Result of the unsigned long type expression if any error occurs during evaluation. Result will be in string format.
pitreferrorresult	<String>	Read-only	Result of the ref type expression if any error occurs during evaluation. Result will be in string format.
pitoffseterrorresult	<String>	Read-only	Result of the expression if any error occurs in calculating offset. Result will be in string format.
pitactionerrorresult	<String>	Read-only	Result of the action if any error occurs in evaluation. Result

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			will be in string format.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/policyevaluation **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/policyevaluation? **args=expression: <String_value> ,action: <String_value> , type:<String_value>, input:<String_value>,**

Use this query-parameter to get policyevaluation resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/config/policyevaluation? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/policyevaluation? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of policyevaluation resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/policyevaluation? **view=summary**

Use this query-parameter to get the summary output of policyevaluation resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/policyevaluation? **pagesize=#no;pageno=#no**

Use this query-parameter to get the policyevaluation resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "policyevaluation": [ {

expression:<String_value>,action:<String_value>,<b>type:<String_value>,</
b><b>input:<String_value>,</b>"pitmodifiedinputdata":<String_value>,

"pitboolresult":<Boolean_value>,

"pitnumresult":<Integer_value>,

"pitdoubleresult":<Double_value>,

"pitulongresult":<Integer_value>,

"pitrefresult":<String_value>,

"pitoffsetresult":<Integer_value>,

"pitoffsetresultlen":<Integer_value>,

"istruncatedrefresult":<Boolean_value>,

"pitboolevaltime":<Integer_value>,

"pitnumevaltime":<Integer_value>,

"pitdoubleevaltime":<Integer_value>,

"pitulongevaltime":<Integer_value>,

"pitrefevaltime":<Integer_value>,

"pitoffsetevaltime":<Integer_value>,

"pitactionevaltime":<Integer_value>,

"pitoperationperformerarray":<String[]_value>,

"pitoldoffsetarray":<Integer[]_value>,
```

```
"pitnewoffsetarray":<Integer[]_value>,

"pitoffsetlengtharray":<Integer[]_value>,

"pitoffsetnewlengtharray":<Integer[]_value>,

"pitboolerrorresult":<String_value>,

"pitnumerrorresult":<String_value>,

"pitdoubleerrorresult":<String_value>,

"pitulongerrorresult":<String_value>,

"pitreferrorresult":<String_value>,

"pitoffseterrorresult":<String_value>,

"pitactionerrorresult":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/policyevaluation? **args=expression: <String_value> ,action: <String_value> , type:<String_value>, input:<String_value>, ;count=yes**
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "policyevaluation": [ { "__count": "#no"} ] }
```

policyexpression

Configuration for expression resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Unique name for the expression. Not case sensitive. Must begin with an ASCII letter or underscore (_) character, and must consist only of ASCII alphanumeric or underscore characters. Must not begin with 're' or 'xp' or be a word reserved for use as an expression qualifier prefix (such as HTTP) or enumeration value (such as ASCII). Must not be the name of an existing named expression, pattern set, dataset, stringmap, or HTTP callout. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
value	<String>	Read-write	Expression string. For example: http.req.body(100).contains("this").
comment	<String>	Read-write	Any comments associated with the expression. Displayed upon viewing the policy expression.
clientsecuritymessage	<String>	Read-write	Message to display if the expression fails. Allowed for classic end-point check expressions only. Minimum length = 1
type	<String>	Read-write	Type of expression. Can be a classic or default syntax (advanced) expression. Possible values = CLASSIC, ADVANCED
hits	<Integer>	Read-only	The total number of hits.
pihits	<Integer>	Read-only	The total number of hits.
type1	<String>	Read-only	The type of expression. This is for output only. Possible values = CLASSIC, ADVANCED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
isdefault	<Boolean>	Read-only	A value of true is returned if it is a default policy expression.
builtin	<String[]>	Read-only	Indicates that a variable is a built-in (SYSTEM INTERNAL) type. Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL
feature	<String>	Read-only	The feature to be checked while applying this config.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/policyexpression **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"policyexpression":{

<b>"name":<String_value>,

</b><b>"value":<String_value>,

</b>"comment":<String_value>,
```

```
"clientsecuritymessage":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/policyexpression/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/policyexpression **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"policyexpression":{

<b>"name":<String_value>,

</b>"value":<String_value>,

"comment":<String_value>,

"clientsecuritymessage":<String_value>
```

```
}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/policyexpression? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"policyexpression":{

<b>"name":<String_value>,

</b>"comment":true,

"clientsecuritymessage":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/policyexpression **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/policyexpression? **args=name: <String_value> ,type: <String_value>**

Use this query-parameter to get policyexpression resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/config/policyexpression? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/policyexpression? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of policyexpression resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/policyexpression? **view=summary**

Use this query-parameter to get the summary output of policyexpression resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/policyexpression? **pagesize=#no;pageno=#no**

Use this query-parameter to get the policyexpression resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "policyexpression": [ {

name:<String_value>,type:<String_value>"value":<String_value>,
```

```
"hits":<Integer_value>,

"pihits":<Integer_value>,

"type1":<String_value>,

"clientsecuritymessage":<String_value>,

"comment":<String_value>,

"isdefault":<Boolean_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/policyexpression/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/policyexpression/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/policyexpression/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of policyexpression resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "policyexpression": [ {

name:<String_value>,type:<String_value>"value":<String_value>,

"hits":<Integer_value>,

"pihits":<Integer_value>,

"type1":<String_value>,

"clientsecuritymessage":<String_value>,

"comment":<String_value>,

"isdefault":<Boolean_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/policyexpression? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "policyexpression": [ { "__count": "#no"} ] }
```

policyhttpcallout

Configuration for HTTP callout resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the HTTP callout. Not case sensitive. Must begin with an ASCII letter or underscore (_) character, and must consist only of ASCII alphanumeric or underscore characters. Must not begin with 're' or 'xp' or be a word reserved for use as an expression qualifier prefix (such as HTTP) or enumeration value (such as ASCII).

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Must not be the name of an existing named expression, pattern set, dataset, stringmap, or HTTP callout. Minimum length = 1
ipaddress	<String>	Read-write	IP Address of the server (callout agent) to which the callout is sent. Can be an IPv4 or IPv6 address. Mutually exclusive with the Virtual Server parameter. Therefore, you cannot set the <IP Address, Port> and the Virtual Server in the same HTTP callout.
port	<Integer>	Read-write	Server port to which the HTTP callout agent is mapped. Mutually exclusive with the Virtual Server parameter. Therefore, you cannot set the <IP Address, Port> and the Virtual Server in the same HTTP callout. Minimum value = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
vserver	<String>	Read-write	Name of the load balancing, content switching, or cache redirection virtual server (the callout agent) to which the HTTP callout is sent. The service type of the virtual server must be HTTP. Mutually exclusive with the IP address and port parameters. Therefore, you cannot set the <IP Address, Port> and the Virtual Server in the same HTTP callout. Minimum length = 1
returntype	<String>	Read-write	Type of data that the target callout agent returns in response to the callout. Available settings function as follows: * TEXT - Treat the returned value as a text string. * NUM - Treat the returned value as a number. * BOOL - Treat the returned value as a Boolean value.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Note: You cannot change the return type after it is set. Possible values = BOOL, NUM, TEXT
httpmethod	<String>	Read-write	Method used in the HTTP request that this callout sends. Mutually exclusive with the full HTTP request expression. Possible values = GET, POST
hostexpr	<String>	Read-write	String expression to configure the Host header. Can contain a literal value (for example, 10.101.10.11) or a derived value (for example, http.req.header("Host")). The literal value can be an IP address or a fully qualified domain name. Mutually exclusive with the full HTTP request expression. Minimum length = 1
urlstemexpr	<String>	Read-write	String expression for generating the URL stem. Can contain a literal string (for example, "/mysite/index.html") or an expression that

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			derives the value (for example, http.req.url). Mutually exclusive with the full HTTP request expression. Minimum length = 1
headers	<String[]>	Read-write	One or more headers to insert into the HTTP request. Each header is specified as "name(expr)", where expr is an expression that is evaluated at runtime to provide the value for the named header. You can configure a maximum of eight headers for an HTTP callout. Mutually exclusive with the full HTTP request expression.
parameters	<String[]>	Read-write	One or more query parameters to insert into the HTTP request URL (for a GET request) or into the request body (for a POST request). Each parameter is specified as "name(expr)", where expr is an expression that is evaluated at run time to provide the value for the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			named parameter (name=value). The parameter values are URL encoded. Mutually exclusive with the full HTTP request expression.
bodyexpr	<String>	Read-write	An advanced string expression for generating the body of the request. The expression can contain a literal string or an expression that derives the value (for example, client.ip.src). Mutually exclusive with -fullReqExpr. Minimum length = 1
fullreqexpr	<String>	Read-write	Exact HTTP request, in the form of an expression, which the Citrix ADC sends to the callout agent. If you set this parameter, you must not include HTTP method, host expression, URL stem expression, headers, or parameters. The request expression is constrained by the feature for which the callout is used.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			For example, an HTTP.RES expression cannot be used in a request-time policy bank or in a TCP content switching policy bank. The Citrix ADC does not check the validity of this request. You must manually validate the request. Minimum length = 1
scheme	<String>	Read-write	Type of scheme for the callout server. Possible values = http, https
resultexpr	<String>	Read-write	Expression that extracts the callout results from the response sent by the HTTP callout agent. Must be a response based expression, that is, it must begin with HTTP.RES. The operations in this expression must match the return type. For example, if you configure a return type of TEXT, the result expression

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			must be a text based expression. If the return type is NUM, the result expression (resultExpr) must return a numeric value, as in the following example: http.res.body(10000).length. Minimum length = 1
cacheforsecs	<Integer>	Read-write	Duration, in seconds, for which the callout response is cached. The cached responses are stored in an integrated caching content group named "calloutContentGroup". If no duration is configured, the callout responses will not be cached unless normal caching configuration is used to cache them. This parameter takes precedence over any normal caching configuration that would otherwise apply to these responses. Note that the calloutContentGroup definition may not be modified or removed nor may it

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			be used with other cache policies. Minimum value = 1 Maximum value = 31536000
comment	<String>	Read-write	Any comments to preserve information about this HTTP callout.
hits	<Integer>	Read-only	Total hits.
undefhits	<Integer>	Read-only	Total undefs.
svrstate	<String>	Read-only	The state of the service. Possible values = UP, DOWN, UNKNOWN, BUSY, OUT OF SERVICE, GOING OUT OF SERVICE, DOWN WHEN GOING OUT OF SERVICE, NS_EMPTY_STR, Unknown, DISABLED
effectivestate	<String>	Read-only	The effective state of the service. Possible values = UP, DOWN, UNKNOWN, BUSY, OUT OF SERVICE, GOING OUT OF SERVICE, DOWN

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			WHEN GOING OUT OF SERVICE, NS_EMPTY_STR, Unknown, DISABLED
undefreason	<String>	Read-only	Reason for last undef. Possible values = Failed to add service, Vserver not found, Not a HTTP or SSL vserver, Generated callout request is invalid, Content-Length header not found in callout request, Not enough space to put Content-Length value, Config incomplete, Server is DOWN, Creating callout connection failed, No memory to generate callout request packets, No memory to create callout task, No memory to create callout async, Callout request expression undef, No callout response expression, Skipped callout response

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			eval, Callout response pixl init undef, Callout response expression undef
recursivecallout	<Integer>	Read-only	Number of recursive callouts.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.
- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of

creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/policyhttpcallout **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"policyhttpcallout":{

<b>"name":<String_value>,

</b>"ipaddress":<String_value>,

"port":<Integer_value>,

"vserver":<String_value>,

"returntype":<String_value>,

"httpmethod":<String_value>,

"hostexpr":<String_value>,

"urlstemexpr":<String_value>,
```

```
"headers":<String[]_value>,

"parameters":<String[]_value>,

"bodyexpr":<String_value>,

"fullreqexpr":<String_value>,

"scheme":<String_value>,

"resultexpr":<String_value>,

"cacheforsecs":<Integer_value>,

"comment":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/policyhttpcallout/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/policyhttpcallout **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"policyhttpcallout":{

<b>"name":<String_value>,

</b>"ipaddress":<String_value>,

"port":<Integer_value>,

"vserver":<String_value>,

"returntype":<String_value>,

"httpmethod":<String_value>,

"hostexpr":<String_value>,

"urlstemexpr":<String_value>,

"headers":<String[]_value>,

"parameters":<String[]_value>,

"bodyexpr":<String_value>,

"fullreqexpr":<String_value>,

"scheme":<String_value>,

"resultexpr":<String_value>,

"cacheforsecs":<Integer_value>,

"comment":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/policyhttpcallout? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"policyhttpcallout":{

<b>"name":<String_value>,

</b>"ipaddress":true,

"port":true,

"vserver":true,

"httpmethod":true,

"hostexpr":true,

"urlstemexpr":true,

"headers":true,

"parameters":true,

"bodyexpr":true,

"fullreqexpr":true,

"resultexpr":true,

"cacheforsecs":true,
```

```
"comment":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/policyhttpcallout **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/policyhttpcallout? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/policyhttpcallout? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of policyhttpcallout resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/policyhttpcallout? **view=summary**

Use this query-parameter to get the summary output of policyhttpcallout resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/policyhttpcallout? **pagesize=#no;pageno=#no**

Use this query-parameter to get the policyhttpcallout resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "policyhttpcallout": [ {

"name":<String_value>,

"ipaddress":<String_value>,

"port":<Integer_value>,

"vserver":<String_value>,

"returntype":<String_value>,

"scheme":<String_value>,

"httpmethod":<String_value>,

"hostexpr":<String_value>,

"urlstemexpr":<String_value>,

"headers":<String[]_value>,

"parameters":<String[]_value>,

"fullreqexpr":<String_value>,

"resultexpr":<String_value>,

"hits":<Integer_value>,

"undefhits":<Integer_value>,

"svrstate":<String_value>,
```

```
"effectivestate":<String_value>,

"undefreason":<String_value>,

"recursivecallout":<Integer_value>,

"bodyexpr":<String_value>,

"cacheforsecs":<Integer_value>,

"comment":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/policyhttpcallout/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/policyhttpcallout/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/policyhttpcallout/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of policyhttpcallout resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "policyhttpcallout": [ {

"name":<String_value>,

"ipaddress":<String_value>,

"port":<Integer_value>,

"vserver":<String_value>,

"returntype":<String_value>,

"scheme":<String_value>,

"httpmethod":<String_value>,

"hostexpr":<String_value>,

"urlstemexpr":<String_value>,

"headers":<String[]_value>,

"parameters":<String[]_value>,

"fullreqexpr":<String_value>,

"resultexpr":<String_value>,

"hits":<Integer_value>,

"undefhits":<Integer_value>,

"svrstate":<String_value>,
```

```
"effectivestate":<String_value>,

"undefreason":<String_value>,

"recursivecallout":<Integer_value>,

"bodyexpr":<String_value>,

"cacheforsecs":<Integer_value>,

"comment":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/policyhttpcallout? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "policyhttpcallout": [ { "__count": "#no"} ] }
```

policymap

Configuration for map policy resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
mappolicyname	<String>	Read-write	Name for the map policy. Must begin with a letter, number, or the underscore (_) character and must consist only of letters, numbers, and the hash (#), period (.), colon (:), space ( ), at (@), equals (=), hyphen (-), and underscore (_) characters. CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my map" or 'my map'). Minimum length = 1
sd	<String>	Read-write	Publicly known source domain name. This is the domain name with which a client request arrives at a reverse proxy virtual server for cache redirection. If you

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			specify a source domain, you must specify a target domain. Minimum length = 1
su	<String>	Read-write	Source URL. Specify all or part of the source URL, in the following format: /[[prefix] [*]] [.suffix]. Minimum length = 1
td	<String>	Read-write	Target domain name sent to the server. The source domain name is replaced with this domain name. Minimum length = 1
tu	<String>	Read-write	Target URL. Specify the target URL in the following format: /[[prefix] [*]][.suffix]. Minimum length = 1
targetname	<String>	Read-only	The expression string.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET (ALL)

- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/policymap **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"policymap":{

<b>"mappolicyname":<String_value>,

</b><b>"sd":<String_value>,

</b>"su":<String_value>,

"td":<String_value>,

"tu":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/policymap/ mappolicyname_value<String>
HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/policymap **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/policymap? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/policymap? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of policymap resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/policymap? **view=summary**

Use this query-parameter to get the summary output of policymap resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/policymap? **pagesize=#no;pageno=#no**

Use this query-parameter to get the policymap resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "policymap": [ {

"mappolicyname":<String_value>,

"sd":<String_value>,

"su":<String_value>,

"td":<String_value>,

"tu":<String_value>,
```

```
"targetname":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/policymap/ mappolicyname_value<String>
Query-parameters: attrs http:// <netscaler-ip-address> /nitro/v1/config/policymap/ mappolicyname_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/policymap/ mappolicyname_value<String> ? **view=summary**

Use this query-parameter to get the summary output of policymap resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "policymap": [ {

"mappolicyname":<String_value>,

"sd":<String_value>,

"su":<String_value>,

"td":<String_value>,

"tu":<String_value>,

"targetname":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/policymap? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "policymap": [ { "__count": "#no"} ] }
```

policyparam

Configuration for policy parameter resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
timeout	<Integer>	Read-write	Maximum time in milliseconds to allow for processing expressions and policies without interruption. If the timeout is reached then the evaluation causes an UNDEF to be raised and no further processing is performed. Default value: 3900 Minimum value = 1 Maximum value = 5000
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- UPDATE
- UNSET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/policyparam **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"policyparam":{

"timeout":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/policyparam? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"policyparam":{

"timeout":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/policyparam **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "policyparam": [ {

"timeout":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

policypatset

Configuration for PAT set resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Unique name of the pattern set. Not case sensitive. Must begin with an ASCII letter or underscore (_) character and must contain only alphanumeric and underscore characters. Must not be the name of an existing named expression, pattern set, dataset, string map, or HTTP callout. Minimum length = 1
comment	<String>	Read-write	Any comments to preserve information about this patset or a

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			pattern bound to this patset.
patsetfile	<String>	Read-write	File which contains list of patterns that needs to be bound to the patset. A patsetfile cannot be associated with multiple patsets.
dynamic	<String>	Read-write	This is used to populate internal patset information so that the patset can also be used dynamically in an expression. Here dynamically means the patset name can also be derived using an expression. For example for a given patset name "allow_test" it can be used dynamically as http.req.url.contains_any("allow_" + http.req.url.path.get(1)). This cannot be used with default patsets. Default value: NO Possible values = YES, NO
dynamiconly	<Boolean>	Read-write	Shows only dynamic patsets when set true. Default value: 0

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/policypatset **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"policypatset":{

<b>"name":<String_value>,

</b>"comment":<String_value>,

"patsetfile":<String_value>,

"dynamic":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/policypatset/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/policypatset **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"policypatset":{

<b>"name":<String_value>,

</b>"dynamic":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/policypatset? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"policypatset":{

<b>"name":<String_value>,
```

```
</b>"dynamic":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/policypatset **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/policypatset? **args=name: <String_value> ,dynamiconly: <Boolean_value>**

Use this query-parameter to get policypatset resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/config/policypatset? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/policypatset? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of policypatset resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/policypatset? **view=summary**

Use this query-parameter to get the summary output of policypatset resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/policypatset? **pagesize=#no;pageno=#no**

Use this query-parameter to get the policypatset resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "policypatset": [ {

name:<String_value>,dynamiconly:<Boolean_value>"comment":<String_value>,

"patsetfile":<String_value>,

"dynamic":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/policypatset/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/policypatset/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/policypatset/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of policypatset resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "policypatset": [ {

name:<String_value>,dynamiconly:<Boolean_value>"comment":<String_value>,

"patsetfile":<String_value>,

"dynamic":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/policypatset? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "policypatset": [ { "__count": "#no"} ] }
```

policypatset_binding

Binding object which returns the resources bound to policypatset.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the pattern set for which to display the detailed information. If a name is not provided, a list of all pattern sets configured on the appliance is shown. Minimum length = 1
policypatset_pattern_binding	<policypatset_pattern_binding[]>	Read-only	pattern that can be bound to policypatset.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/policypatset_binding/ name_value<String>
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "policypatset_binding": [ {

"name":<String_value>,

"policypatset_pattern_binding":<policypatset_pattern_binding[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/policypatset_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/policypatset_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "policypatset_binding": [ {

"name":<String_value>,
```

```
"policypatset_pattern_binding":<policypatset_pattern_binding[]_value>

}]}
```

policypatset_pattern_binding

Binding object showing the pattern that can be bound to policypatset.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
charset	<String>	Read-write	Character set associated with the characters in the string. Note: UTF-8 characters can be entered directly (if the UI supports it) or can be encoded as a sequence of hexadecimal bytes '\xNN'. For example, the UTF-8 character ' ' can be encoded as '\xC3\xBC'. Possible values = ASCII, UTF_8
builtin	<String[]>	Read-write	Indicates that a variable is a built-in (SYSTEM INTERNAL) type. Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
comment	<String>	Read-write	Any comments to preserve information about this patset or a pattern bound to this patset.
String	<String>	Read-write	String of characters that constitutes a pattern. For more information about the characters that can be used, refer to the character set parameter. Note: Minimum length for pattern sets used in rewrite actions of type REPLACE_ALL, DELETE_ALL, INSERT_AFTER_ALL, and INSERT_BEFORE_ALL, is three characters.
feature	<String>	Read-write	The feature to be checked while applying this config.
name	<String>	Read-write	Name of the pattern set to which to bind the string. Minimum length = 1
index	<Integer>	Read-write	The index of the string associated with the patset.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/policypatset_pattern_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"policypatset_pattern_binding":{

<b>"name":<String_value>,

</b><b>"String":<String_value>,

</b>"index":<Integer_value>,

"charset":<String_value>,

"comment":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/policypatset_pattern_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ policypatset_pattern_binding/ name_value<String> ? **args= String:<String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/policypatset_pattern_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ policypatset_pattern_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of policypatset_pattern_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/policypatset_pattern_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the policypatset_pattern_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "policypatset_pattern_binding": [ {

"charset":<String_value>,

"builtin":<String[]_value>,

"comment":<String_value>,

"String":<String_value>,

"feature":<String_value>,
```

```
"name":<String_value>,

"index":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/policypatset_pattern_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/policypatset_pattern_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "policypatset_pattern_binding": [ {

"charset":<String_value>,

"builtin":<String[]_value>,

"comment":<String_value>,
```

```
"String":<String_value>,

"feature":<String_value>,

"name":<String_value>,

"index":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/policypatset_pattern_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"policypatset_pattern_binding": [ { "__count": "#no"} ] }
```

policypatsetfile

Configuration for patset file resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
src	<String>	Read-write	URL in protocol, host, path, and file name format from where the patset file will be imported. If file is already present, then it can be imported using local keyword (import patsetfile local:filename patsetfile1) NOTE: The import fails if the object to be imported is on an HTTPS server that requires client certificate authentication for access. Minimum length = 1 Maximum length = 2047
name	<String>	Read-write	Name to assign to the imported patset file. Unique name of the pattern set. Not case sensitive. Must begin with an ASCII letter or underscore (_) character and must contain only alphanumeric and underscore characters. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum length = 31
overwrite	<Boolean>	Read-write	Overwrites the existing file.
delimiter	<String>	Read-write	patset file patterns delimiter. Default value: 10
charset	<String>	Read-write	Character set associated with the characters in the string. Possible values = ASCII, UTF_8
comment	<String>	Read-write	Any comments to preserve information about this patsetfile.
imported	<Boolean>	Read-write	When set, display only shows all imported patsetfiles. Default value: 0
totalpatterns	<Integer>	Read-only	Total number of patterns in the patset file.
boundpatterns	<Integer>	Read-only	Total number of patterns bound to a patset.
patsetname	<String>	Read-only	The patset with which the patsetfile is associated.
bindstatuscode	<Integer>	Read-only	The status code of pattern bindings to patset.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
bindstatus	<String>	Read-only	The status of pattern bindings to patset.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- IMPORT
- ADD
- DELETE
- CHANGE
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

IMPORT

URL: http:// <netscaler-ip-address> /nitro/v1/config/policypatsetfile? **action=Import HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"policypatsetfile":{

<b>"src":<String_value>,

</b><b>"name":<String_value>,

</b>"overwrite":<Boolean_value>,

"delimiter":<String_value>,

"charset":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/policypatsetfile **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"policypatsetfile":{

<b>"name":<String_value>,

</b>"comment":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/policypatsetfile/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

CHANGE

URL: http:// <netscaler-ip-address> /nitro/v1/config/policypatsetfile? **action=update HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"policypatsetfile":{

<b>"name":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/policypatsetfile **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/policypatsetfile? **args=name: <String_value> ,imported: <Boolean_value>**

Use this query-parameter to get policypatsetfile resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/config/policypatsetfile? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/policypatsetfile? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of policypatsetfile resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/policypatsetfile? **view=summary**

Use this query-parameter to get the summary output of policypatsetfile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/policypatsetfile? **pagesize=#no;pageno=#no**

Use this query-parameter to get the policypatsetfile resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "policypatsetfile": [ {

name:<String_value>,imported:<Boolean_value>"src":<String_value>,

"delimiter":<String_value>,

"charset":<String_value>,

"totalpatterns":<Integer_value>,

"boundpatterns":<Integer_value>,

"patsetname":<String_value>,

"comment":<String_value>,

"bindstatuscode":<Integer_value>,

"bindstatus":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/policypatsetfile/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/policypatsetfile/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/policypatsetfile/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of policypatsetfile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "policypatsetfile": [ {

name:<String_value>,imported:<Boolean_value>"src":<String_value>,

"delimiter":<String_value>,

"charset":<String_value>,

"totalpatterns":<Integer_value>,
```

```
"boundpatterns":<Integer_value>,

"patsetname":<String_value>,

"comment":<String_value>,

"bindstatuscode":<Integer_value>,

"bindstatus":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/policypatsetfile? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "policypatsetfile": [ { "__count": "#no"} ] }
```

policystringmap

Configuration for string map resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Unique name for the string map. Not case sensitive. Must begin with an ASCII letter or underscore (_) character, and must consist only of ASCII alphanumeric or underscore characters. Must not begin with 're' or 'xp' or be a word reserved for use as an expression qualifier prefix (such as HTTP) or enumeration value (such as ASCII). Must not be the name of an existing named expression, pattern set, dataset, string map, or HTTP callout. Minimum length = 1
comment	<String>	Read-write	Comments associated with the string map or key-value pair bound to this string map.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/policystringmap **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"policystringmap":{

<b>"name":<String_value>,

</b>"comment":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/policystringmap/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/policystringmap **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"policystringmap":{

<b>"name":<String_value>,

</b>"comment":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/policystringmap? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"policystringmap":{

<b>"name":<String_value>,

</b>"comment":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/policystringmap **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/policystringmap? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/policystringmap? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of policystringmap resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/policystringmap? **view=summary**

Use this query-parameter to get the summary output of policystringmap resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/policystringmap? **pagesize=#no;pageno=#no**

Use this query-parameter to get the policystringmap resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "policystringmap": [ {

"name":<String_value>,

"comment":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/policystringmap/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/policystringmap/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/policystringmap/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of policystringmap resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "policystringmap": [ {

"name":<String_value>,

"comment":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/policystringmap? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "policystringmap": [ { "__count": "#no"} ] }
```

policystringmap_binding

Binding object which returns the resources bound to policystringmap.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the string map to display. If a name is not provided, a list of all the configured string maps is shown. Minimum length = 1
policystringmap_pattern_binding	<policystringmap_pattern_binding[]>	Read-only	pattern that can be bound to policystringmap.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/policystringmap_binding/ name_value<String>
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "policystringmap_binding": [ {

"name":<String_value>,

"policystringmap_pattern_binding":<policystringmap_pattern_binding[]_value
>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/policystringmap_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/policystringmap_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "policystringmap_binding": [ {

"name":<String_value>,

"policystringmap_pattern_binding":<policystringmap_pattern_binding[]_value
>

}]}
```

policystringmap_pattern_binding

Binding object showing the pattern that can be bound to policystringmap.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the string map to which to bind the key-value pair. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
key	<String>	Read-write	Character string constituting the key to be bound to the string map. The key is matched against the data processed by the operation that uses the string map. The default character set is ASCII. UTF-8 characters can be included if the character set is UTF-8. UTF-8 characters can be entered directly (if the UI supports it) or can be encoded as a sequence of hexadecimal bytes '\xNN'. For example, the UTF-8 character '' can be encoded as '\xC3\xBC'. Minimum length = 1
value	<String>	Read-write	Character string constituting the value associated with the key. This value is returned when processed data matches the associated key. Refer to the key parameter for details of the value character set. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
comment	<String>	Read-write	Comments associated with the string map or key-value pair bound to this string map.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/policystringmap_pattern_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"policystringmap_pattern_binding":{

<b>"name":<String_value>,

</b><b>"key":<String_value>,

</b><b>"value":<String_value>,

</b>"comment":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/policystringmap_pattern_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ policystringmap_pattern_binding/ name_value<String> ? **args= key:<String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/policystringmap_pattern_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ policystringmap_pattern_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of policystringmap_pattern_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/policystringmap_pattern_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the policystringmap_pattern_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "policystringmap_pattern_binding": [ {

"name":<String_value>,

"key":<String_value>,

"value":<String_value>,

"comment":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/policystringmap_pattern_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/policystringmap_pattern_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "policystringmap_pattern_binding": [ {

"name":<String_value>,

"key":<String_value>,

"value":<String_value>,

"comment":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/policystringmap_pattern_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"policystringmap_pattern_binding": [ { "__count": "#no"} ] }
```

policytracing

Configuration for 0 resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
filterexpr	<String>	Read-write	Policy tracing filter expression. For example: http.req.url.startswith ("/this").
protocoltype	<String>	Read-write	protocol type for which policy records needs to be collected. Default value: HTTP Possible values = HTTP, SSL, TCP, SSL_TCP, DNS, DNS_TCP, ANY
capturesslhandshake policies	<String>	Read-write	Set it to yes if need to capture the SSL handshake policies. Default value: NO Possible values = YES, NO
transactionid	<String>	Read-write	Unique ID to identify the current transaction.
detail	<String>	Read-write	Show detailed information of the captured records. Default value: all Possible values = brief, all
nodeid	<Integer>	Read-write	Unique number that identifies the cluster node.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum value = 0 Maximum value = 31
packetengineid	<Integer>	Read-only	The packet engine identifier.
clientip	<String>	Read-only	The IP address of client.
destip	<String>	Read-only	The IP address of destination.
srcport	<Integer>	Read-only	Source port of the request.
destport	<Integer>	Read-only	Destination port of the request.
transactiontime	<String>	Read-only	Conveys time at which request processing started.
policytracingmodule	<String>	Read-only	Module or feature for which policy is evaluated. Possible values = SSL, DNS, DNS64, VPNTraffic, VPNSession, VPNURL, VPNApp, TMTraffic, TMSession, SAMLIdp, Authentication, Authorizaion, CacheRedirection, ContentSwitching, Bot Management,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			AppFw, ContentInspection, Responder, ContentOptimization, Video Optimization, CACHE, REWRITE, AppQoE, AppFlow, LB, Compression, TunnelTraffic, URLTRANS, CVPNRewrite
url	<String>	Read-only	Request URL.
policynames	<String[]>	Read-only	List of the policy names which are evaluated to true for this transaction.
isresponse	<Integer>	Read-only	True if the current policy is evaluated on the request side.
isundefpolicy	<Integer>	Read-only	True if the current policy is evaluated to undef.
policytracingrecordcount	<Integer>	Read-only	Current record number.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- START

- STOP
- CLEAR
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

START

URL: http:// <netscaler-ip-address> /nitro/v1/config/policytracing? **action=start HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"policytracing":{

<b>"filterexpr":<String_value>,

</b>"protocoltype":<String_value>,

"capturesslhandshakepolicies":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

STOP

URL: http:// <netscaler-ip-address> /nitro/v1/config/policytracing? **action=stop HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"policytracing":{

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

CLEAR

URL: http:// <netscaler-ip-address> /nitro/v1/config/policytracing? **action=clear HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"policytracing":{

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/policytracing **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/policytracing? **args=transactionid: <String_value> ,detail: <String_value> ,nodeid: <Integer_value>**

Use this query-parameter to get policytracing resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/config/policytracing? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/policytracing? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of policytracing resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/policytracing? **view=summary**

Use this query-parameter to get the summary output of policytracing resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/policytracing? **pagesize=#no;pageno=#no**

Use this query-parameter to get the policytracing resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "policytracing": [ {

transactionid:<String_value>,detail:<String_value>,nodeid:<Integer_value>"
filterexpr":<String_value>,

"transactionid":<String_value>,

"packetengineid":<Integer_value>,

"clientip":<String_value>,

"destip":<String_value>,

"srcport":<Integer_value>,

"destport":<Integer_value>,
```

```
"transactiontime":<String_value>,

"policytracingmodule":<String_value>,

"url":<String_value>,

"policynames":<String[]_value>,

"isresponse":<Integer_value>,

"isundefpolicy":<Integer_value>,

"policytracingrecordcount":<Integer_value>,

"protocoltype":<String_value>,

"capturesslhandshakepolicies":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/policytracing? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "policytracing": [ { "__count": "#no"} ] }
```

policyurlset

Configuration for URL set resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Unique name of the url set. Not case sensitive. Must begin with an ASCII letter or underscore (_) character and must contain only alphanumeric and underscore characters. Must not be the name of an existing named expression, pattern set, dataset, string map, or HTTP callout. Minimum length = 1 Maximum length = 127
comment	<String>	Read-write	Any comments to preserve information about this url set.
imported	<Boolean>	Read-write	when set, display shows all imported urlsets. Default value: 0

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
overwrite	<Boolean>	Read-write	Overwrites the existing file. Default value: 0
delimiter	<String>	Read-write	CSV file record delimiter. Default value: 44
rowseparator	<String>	Read-write	CSV file row separator. Default value: 10
url	<String>	Read-write	URL (protocol, host, path and file name) from where the CSV (comma separated file) file will be imported or exported. Each record/line will one entry within the urlset. The first field contains the URL pattern, subsequent fields contains the metadata, if available. HTTP, HTTPS and FTP protocols are supported. NOTE: The operation fails if the destination HTTPS server requires client certificate authentication for access. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum length = 2047
interval	<Integer>	Read-write	The interval, in seconds, rounded down to the nearest 15 minutes, at which the update of urlset occurs. Default value: 0 Minimum value = 0 Maximum value = 2592000
privateset	<Boolean>	Read-write	Prevent this urlset from being exported. Default value: 0
subdomainexactmatch	<Boolean>	Read-write	Force exact subdomain matching, ex. given an entry 'google.com' in the urlset, a request to 'news.google.com' won't match, if subdomainExactMatch is set. Default value: 0
matchedid	<Integer>	Read-write	An ID that would be sent to AppFlow to indicate which URLSet was the last one that matched the requested URL. Default value: 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum value = 2 Maximum value = 31
canaryurl	<String>	Read-write	Add this URL to this urlset. Used for testing when contents of urlset is kept confidential. Minimum length = 1 Maximum length = 2047
patterncount	<Integer>	Read-only	Number of patterns in this urlset. Default value: 0
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET (ALL)
- GET
- COUNT
- IMPORT
- CHANGE
- EXPORT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/policyurlset **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"policyurlset":{

<b>"name":<String_value>,

</b>"comment":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/policyurlset/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

IMPORT

URL: http:// <netscaler-ip-address> /nitro/v1/config/policyurlset? **action=Import HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"policyurlset":{

<b>"name":<String_value>,

</b>"overwrite":<Boolean_value>,

"delimiter":<String_value>,

"rowseparator":<String_value>,

<b>"url":<String_value>,
```

```
</b>"interval":<Integer_value>,

"privateset":<Boolean_value>,

"subdomainexactmatch":<Boolean_value>,

"matchedid":<Integer_value>,

"canaryurl":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

CHANGE

URL: http:// <netscaler-ip-address> /nitro/v1/config/policyurlset? **action=update HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"policyurlset":{

<b>"name":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

EXPORT

URL: http:// <netscaler-ip-address> /nitro/v1/config/policyurlset? **action=export HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"policyurlset":{

<b>"name":<String_value>,

</b><b>"url":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/policyurlset **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/policyurlset? **args=name: <String_value> ,imported: <Boolean_value>**

Use this query-parameter to get policyurlset resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/config/policyurlset? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/policyurlset? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of policyurlset resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/policyurlset? **view=summary**

Use this query-parameter to get the summary output of policyurlset resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/policyurlset? **pagesize=#no;pageno=#no**

Use this query-parameter to get the policyurlset resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "policyurlset": [ {

name:<String_value>,imported:<Boolean_value>"comment":<String_value>,

"patterncount":<Integer_value>,

"url":<String_value>,

"delimiter":<String_value>,

"rowseparator":<String_value>,

"interval":<Integer_value>,
```

```
"matchedid":<Integer_value>,

"canaryurl":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/policyurlset/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/policyurlset/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/policyurlset/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of policyurlset resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "policyurlset": [ {

name:<String_value>,imported:<Boolean_value>"comment":<String_value>,

"patterncount":<Integer_value>,

"url":<String_value>,

"delimiter":<String_value>,

"rowseparator":<String_value>,

"interval":<Integer_value>,

"matchedid":<Integer_value>,

"canaryurl":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/policyurlset? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "policyurlset": [ { "__count": "#no"} ] }
```

protocol

Protocol

Protocol Configuration.

NAME	DESCRIPTION
protocolhttpband	Configuration for HTTP request/response band

protocolhttpband

Configuration for HTTP request/response band resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
reqbandsize	<Integer>	Read-write	Band size, in bytes, for HTTP request band statistics. For example, if you specify a band size of 100 bytes, statistics will be maintained and displayed for the following size ranges: 0 - 99 bytes 100 - 199 bytes 200 - 299 bytes and so on.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: 100 Minimum value = 50
respbandsize	<Integer>	Read-write	Band size, in bytes, for HTTP response band statistics. For example, if you specify a band size of 100 bytes, statistics will be maintained and displayed for the following size ranges: 0 - 99 bytes 100 - 199 bytes 200 - 299 bytes and so on. Default value: 1024 Minimum value = 50
type	<String>	Read-write	Type of statistics to display. Possible values = REQUEST, RESPONSE, MQTT_JUMBO_REQ
nodeid	<Integer>	Read-write	Unique number that identifies the cluster node. Minimum value = 0 Maximum value = 31

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
bandrange	<Integer>	Read-only	The range of the HTTP request/ response size, in bytes.
numberofbands	<Integer>	Read-only	The total number of http bands.
totalbandsize	<Integer[]>	Read-only	The total size of all HTTP requests/ responses in this size range.
avgbandsize	<Integer[]>	Read-only	The average size of all HTTP requests/ responses in this size range.
avgbandsizenew	<Double[]>	Read-only	The average size of all HTTP requests/ responses in this size range.
banddata	<Integer[]>	Read-only	The total size of all HTTP requests/ responses in this size range, expressed as a percentage of the total size of all HTTP requests/responses.
banddatanew	<Double[]>	Read-only	The total size of all HTTP requests/ responses in this size range, expressed as a percentage of the total size of all HTTP requests/responses.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
accesscount	<Integer[]>	Read-only	The number of HTTP requests/responses in this size range.
accessratio	<Integer[]>	Read-only	The number of HTTP requests/responses in this size range, expressed as a percentage of the total number of HTTP requests/responses.
accessrationew	<Double[]>	Read-only	The number of HTTP requests/responses in this size range, expressed as a percentage of the total number of HTTP requests/responses.
totals	<Integer[]>	Read-only	The total of totalBandSize, avgBandSize, BandData, accessCount, accessRatio respectively.
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- UPDATE
- UNSET
- GET (ALL)
- CLEAR

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/protocolhttpband **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"protocolhttpband":{

"reqbandsize":<Integer_value>,

"respbandsize":<Integer_value>
```

```
}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/protocolhttpband? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"protocolhttpband":{

"reqbandsize":true,

"respbandsize":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

CLEAR

URL: http:// <netscaler-ip-address> /nitro/v1/config/protocolhttpband? **action=clear HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"protocolhttpband":{

<b>"type":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/protocolhttpband **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/protocolhttpband? **args= type:<String_value>, nodeid: <Integer_value>**

Use this query-parameter to get protocolhttpband resources based on additional properties.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "protocolhttpband": [ {

<b>type:<String_value>,</
b>nodeid:<Integer_value>"bandrange":<Integer_value>,

"numberofbands":<Integer_value>,

"totalbandsize":<Integer[]_value>,

"avgbandsize":<Integer[]_value>,

"avgbandsizenew":<Double[]_value>,

"banddata":<Integer[]_value>,

"banddatanew":<Double[]_value>,

"accesscount":<Integer[]_value>,

"accessratio":<Integer[]_value>,

"accessrationew":<Double[]_value>,

"totals":<Integer[]_value>,

"reqbandsize":<Integer_value>,

"respbandsize":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

quic

Quic

QUIC configuration.

NAME	DESCRIPTION
quicparam	Configuration for Citrix ADC QUIC parameters
quicprofile	Configuration for QUIC profile

quicparam

Configuration for Citrix ADC QUIC parameters resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
quicsecrettimeout	<Integer>	Read-write	Rotation frequency, in seconds, for the secret used to generate address validation tokens that will be issued in QUIC Retry packets and QUIC NEW_TOKEN frames sent by the Citrix ADC. A value of 0 can be configured if secret rotation is not desired. Default value: 3600 Minimum value = 0 Maximum value = 31536000
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- UPDATE
- UNSET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/quicparam **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"quicparam":{

"quicsecrettimeout":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/quicparam? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"quicparam":{

"quicsecrettimeout":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/quicparam **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "quicparam": [ {

"quicsecrettimeout":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

quicprofile

Configuration for QUIC profile resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the QUIC profile. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			colon (:), at (@),equals sign (=), and hyphen (-) characters. Cannot be changed after the profile is created. Minimum length = 1 Maximum length = 256
ackdelayexponent	<Integer>	Read-write	An integer value advertised by the Citrix ADC to the remote QUIC endpoint, indicating an exponent that the remote QUIC endpoint should use, to decode the ACK Delay field in QUIC ACK frames sent by the Citrix ADC. Default value: 3 Minimum value = 0 Maximum value = 20
activeconnectionidlimit	<Integer>	Read-write	An integer value advertised by the Citrix ADC to the remote QUIC endpoint, specifying the maximum number of QUIC connection IDs from the remote QUIC endpoint, that the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Citrix ADC is willing to store. Default value: 3 Minimum value = 2 Maximum value = 8
activeconnectionmigration	<String>	Read-write	Specify whether the Citrix ADC should allow the remote QUIC endpoint to perform active QUIC connection migration. Default value: ENABLED Possible values = ENABLED, DISABLED
congestionctrlalgorithm	<String>	Read-write	Specify the congestion control algorithm to be used for QUIC connections. The default congestion control algorithm is CUBIC. Default value: Default Possible values = Default, NewReno, CUBIC, BBR
initialmaxdata	<Integer>	Read-write	An integer value advertised by the Citrix ADC to the remote QUIC

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			endpoint, specifying the initial value, in bytes, for the maximum amount of data that can be sent on a QUIC connection. Default value: 1048576 Minimum value = 8192 Maximum value = 67108864
initialmaxstreamdata bidilocal	<Integer>	Read-write	An integer value advertised by the Citrix ADC to the remote QUIC endpoint, specifying the initial flow control limit, in bytes, for bidirectional QUIC streams initiated by the Citrix ADC. Default value: 262144 Minimum value = 8192 Maximum value = 8388608
initialmaxstreamdata bidiremote	<Integer>	Read-write	An integer value advertised by the Citrix ADC to the remote QUIC endpoint, specifying the initial flow control

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			limit, in bytes, for bidirectional QUIC streams initiated by the remote QUIC endpoint. Default value: 262144 Minimum value = 8192 Maximum value = 8388608
initialmaxstreamdatauni	<Integer>	Read-write	An integer value advertised by the Citrix ADC to the remote QUIC endpoint, specifying the initial flow control limit, in bytes, for unidirectional streams initiated by the remote QUIC endpoint. Default value: 262144 Minimum value = 8192 Maximum value = 8388608
initialmaxstreamsbidi	<Integer>	Read-write	An integer value advertised by the Citrix ADC to the remote QUIC endpoint, specifying the initial maximum number of

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			bidirectional streams the remote QUIC endpoint may initiate. Default value: 100 Minimum value = 1 Maximum value = 500
initialmaxstreamsuni	<Integer>	Read-write	An integer value advertised by the Citrix ADC to the remote QUIC endpoint, specifying the initial maximum number of unidirectional streams the remote QUIC endpoint may initiate. Default value: 10 Minimum value = 1 Maximum value = 500
maxackdelay	<Integer>	Read-write	An integer value advertised by the Citrix ADC to the remote QUIC endpoint, specifying the maximum amount of time, in milliseconds, by which the Citrix ADC will delay sending acknowledgments. Default value: 20

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum value = 10 Maximum value = 2000
maxidletimeout	<Integer>	Read-write	An integer value advertised by the Citrix ADC to the remote QUIC endpoint, specifying the maximum idle timeout, in seconds, for a QUIC connection. A QUIC connection will be silently discarded by the Citrix ADC if it remains idle for longer than the minimum of the idle timeout values advertised by the Citrix ADC and the remote QUIC endpoint, and three times the current Probe Timeout (PTO). Default value: 180 Minimum value = 1 Maximum value = 3600
maxudpdatagramsperburst	<Integer>	Read-write	An integer value, specifying the maximum number of UDP datagrams that can be transmitted by the Citrix ADC in

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			a single transmission burst on a QUIC connection. Default value: 8 Minimum value = 1 Maximum value = 256
maxudppayloadsize	<Integer>	Read-write	An integer value advertised by the Citrix ADC to the remote QUIC endpoint, specifying the size of the largest UDP datagram payload, in bytes, that the Citrix ADC is willing to receive on a QUIC connection. Default value: 1472 Minimum value = 1252 Maximum value = 9188
newtokenvalidityperiod	<Integer>	Read-write	An integer value, specifying the validity period, in seconds, of address validation tokens issued through QUIC NEW_TOKEN frames sent by the Citrix ADC. Default value: 300

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum value = 1 Maximum value = 3600
retrytokenvalidityperiod	<Integer>	Read-write	An integer value, specifying the validity period, in seconds, of address validation tokens issued through QUIC Retry packets sent by the Citrix ADC. Default value: 10 Minimum value = 1 Maximum value = 120
statelessaddressvalidation	<String>	Read-write	Specify whether the Citrix ADC should perform stateless address validation for QUIC clients, by sending tokens in QUIC Retry packets during QUIC connection establishment, and by sending tokens in QUIC NEW_TOKEN frames after QUIC connection establishment. Default value: ENABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ENABLED, DISABLED
refcnt	<Integer>	Read-only	Number of entities using this profile.
builtin	<String[]>	Read-only	Flag to determine if the QUIC profile is built-in or not. Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL
feature	<String>	Read-only	The feature to be checked while applying this config.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/quicprofile **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"quicprofile":{

<b>"name":<String_value>,

</b>"ackdelayexponent":<Integer_value>,

"activeconnectionidlimit":<Integer_value>,
```

```
"activeconnectionmigration":<String_value>,

"congestionctrlalgorithm":<String_value>,

"initialmaxdata":<Integer_value>,

"initialmaxstreamdatabidilocal":<Integer_value>,

"initialmaxstreamdatabidiremote":<Integer_value>,

"initialmaxstreamdatauni":<Integer_value>,

"initialmaxstreamsbidi":<Integer_value>,

"initialmaxstreamsuni":<Integer_value>,

"maxackdelay":<Integer_value>,

"maxidletimeout":<Integer_value>,

"maxudpdatagramsperburst":<Integer_value>,

"maxudppayloadsize":<Integer_value>,

"newtokenvalidityperiod":<Integer_value>,

"retrytokenvalidityperiod":<Integer_value>,

"statelessaddressvalidation":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/quicprofile/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/quicprofile **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"quicprofile":{

<b>"name":<String_value>,

</b>"ackdelayexponent":<Integer_value>,

"activeconnectionidlimit":<Integer_value>,

"activeconnectionmigration":<String_value>,

"congestionctrlalgorithm":<String_value>,

"initialmaxdata":<Integer_value>,

"initialmaxstreamdatabidilocal":<Integer_value>,

"initialmaxstreamdatabidiremote":<Integer_value>,

"initialmaxstreamdatauni":<Integer_value>,

"initialmaxstreamsbidi":<Integer_value>,

"initialmaxstreamsuni":<Integer_value>,
```

```
"maxackdelay":<Integer_value>,

"maxidletimeout":<Integer_value>,

"maxudpdatagramsperburst":<Integer_value>,

"maxudppayloadsize":<Integer_value>,

"newtokenvalidityperiod":<Integer_value>,

"retrytokenvalidityperiod":<Integer_value>,

"statelessaddressvalidation":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/quicprofile? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"quicprofile":{

<b>"name":<String_value>,

</b>"ackdelayexponent":true,

"activeconnectionidlimit":true,
```

```
"activeconnectionmigration":true,

"congestionctrlalgorithm":true,

"initialmaxdata":true,

"initialmaxstreamdatabidilocal":true,

"initialmaxstreamdatabidiremote":true,

"initialmaxstreamdatauni":true,

"initialmaxstreamsbidi":true,

"initialmaxstreamsuni":true,

"maxackdelay":true,

"maxidletimeout":true,

"maxudpdatagramsperburst":true,

"maxudppayloadsize":true,

"newtokenvalidityperiod":true,

"retrytokenvalidityperiod":true,

"statelessaddressvalidation":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/quicprofile **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/quicprofile? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/quicprofile? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of quicprofile resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/quicprofile? **view=summary**

Use this query-parameter to get the summary output of quicprofile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/quicprofile? **pagesize=#no;pageno=#no**

Use this query-parameter to get the quicprofile resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "quicprofile": [ {

"name":<String_value>,

"ackdelayexponent":<Integer_value>,

"activeconnectionidlimit":<Integer_value>,
```

```
"activeconnectionmigration":<String_value>,

"congestionctrlalgorithm":<String_value>,

"initialmaxdata":<Integer_value>,

"initialmaxstreamdatabidilocal":<Integer_value>,

"initialmaxstreamdatabidiremote":<Integer_value>,

"initialmaxstreamdatauni":<Integer_value>,

"initialmaxstreamsbidi":<Integer_value>,

"initialmaxstreamsuni":<Integer_value>,

"maxackdelay":<Integer_value>,

"maxidletimeout":<Integer_value>,

"maxudpdatagramsperburst":<Integer_value>,

"maxudppayloadsize":<Integer_value>,

"newtokenvalidityperiod":<Integer_value>,

"retrytokenvalidityperiod":<Integer_value>,

"statelessaddressvalidation":<String_value>,

"refcnt":<Integer_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/quicprofile/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/quicprofile/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/quicprofile/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of quicprofile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "quicprofile": [ {

"name":<String_value>,

"ackdelayexponent":<Integer_value>,

"activeconnectionidlimit":<Integer_value>,

"activeconnectionmigration":<String_value>,
```

```
"congestionctrlalgorithm":<String_value>,

"initialmaxdata":<Integer_value>,

"initialmaxstreamdatabidilocal":<Integer_value>,

"initialmaxstreamdatabidiremote":<Integer_value>,

"initialmaxstreamdatauni":<Integer_value>,

"initialmaxstreamsbidi":<Integer_value>,

"initialmaxstreamsuni":<Integer_value>,

"maxackdelay":<Integer_value>,

"maxidletimeout":<Integer_value>,

"maxudpdatagramsperburst":<Integer_value>,

"maxudppayloadsize":<Integer_value>,

"newtokenvalidityperiod":<Integer_value>,

"retrytokenvalidityperiod":<Integer_value>,

"statelessaddressvalidation":<String_value>,

"refcnt":<Integer_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/quicprofile? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "quicprofile": [ { "__count": "#no"} ] }
```

quicbridge

QuicBridge

QUIC Bridge configuration.

NAME	DESCRIPTION
quicbridgeprofile	Configuration for QUIC BRIDGE profile

quicbridgeprofile

Configuration for QUIC BRIDGE profile resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the QUIC profile. Must begin with an ASCII alphanumeric or

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@),equals sign (=), and hyphen (-) characters. Cannot be changed after the profile is created. Minimum length = 1 Maximum length = 255
routingalgorithm	<String>	Read-write	Routing algorithm to generate routable connection IDs. Default value: PLAINTEXT Possible values = PLAINTEXT
serveridlength	<Integer>	Read-write	Length of serverid to encode/decode server information. Default value: 4 Minimum value = 2 Maximum value = 38
refcnt	<Integer>	Read-only	Number of entities using this profile.
_nextgenapiresource	<String>	Read-only	.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- GET (ALL)
- GET
- COUNT
- UNSET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/quicbridgeprofile **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"quicbridgeprofile":{

<b>"name":<String_value>,

</b>"routingalgorithm":<String_value>,

"serveridlength":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/quicbridgeprofile/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/quicbridgeprofile **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"quicbridgeprofile":{

<b>"name":<String_value>,

</b>"routingalgorithm":<String_value>,

"serveridlength":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/quicbridgeprofile? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"quicbridgeprofile":{

<b>"name":<String_value>,

</b>"routingalgorithm":true,

"serveridlength":true
```

```
}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/quicbridgeprofile **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/quicbridgeprofile? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/quicbridgeprofile? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of quicbridgeprofile resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/quicbridgeprofile? **view=summary**

Use this query-parameter to get the summary output of quicbridgeprofile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/quicbridgeprofile? **pagesize=#no;pageno=#no**

Use this query-parameter to get the quicbridgeprofile resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "quicbridgeprofile": [ {

"name":<String_value>,

"routingalgorithm":<String_value>,

"serveridlength":<Integer_value>,

"refcnt":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/quicbridgeprofile/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/quicbridgeprofile/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/quicbridgeprofile/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of quicbridgeprofile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "quicbridgeprofile": [ {

"name":<String_value>,

"routingalgorithm":<String_value>,

"serveridlength":<Integer_value>,

"refcnt":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/quicbridgeprofile? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "quicbridgeprofile": [ { "__count": "#no"} ] }
```

rdp

Rdp

RDP configuration.

NAME	DESCRIPTION
rdpclientprofile	Configuration for RDP clientprofile
rdpconnections	Configuration for active rdp connections
rdpserverprofile	Configuration for RDP serverprofile

rdpclientprofile

Configuration for RDP clientprofile resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	The name of the rdp profile. Minimum length = 1
rdpurloverride	<String>	Read-write	This setting determines whether the RDP parameters supplied in the vpn

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			url override those specified in the RDP profile. Default value: ENABLE Possible values = ENABLE, DISABLE
redirectclipboard	<String>	Read-write	This setting corresponds to the Clipboard check box on the Local Resources tab under Options in RDC. Default value: ENABLE Possible values = ENABLE, DISABLE
redirectdrives	<String>	Read-write	This setting corresponds to the selections for Drives under More on the Local Resources tab under Options in RDC. Default value: DISABLE Possible values = ENABLE, DISABLE
redirectprinters	<String>	Read-write	This setting corresponds to the selection in the Printers check box on the Local

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Resources tab under Options in RDC. Default value: ENABLE Possible values = ENABLE, DISABLE
redirectcomports	<String>	Read-write	This setting corresponds to the selections for comports under More on the Local Resources tab under Options in RDC. Default value: DISABLE Possible values = ENABLE, DISABLE
redirectpnpdevices	<String>	Read-write	This setting corresponds to the selections for pnpdevices under More on the Local Resources tab under Options in RDC. Default value: DISABLE Possible values = ENABLE, DISABLE
keyboardhook	<String>	Read-write	This setting corresponds to the selection in the Keyboard drop-down list on the Local

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Resources tab under Options in RDC. Default value: InFullScreenMode Possible values = OnLocal, OnRemote, InFullScreenMode
audiocapturemode	<String>	Read-write	This setting corresponds to the selections in the Remote audio area on the Local Resources tab under Options in RDC. Default value: DISABLE Possible values = ENABLE, DISABLE
videoplaybackmode	<String>	Read-write	This setting determines if Remote Desktop Connection (RDC) will use RDP efficient multimedia streaming for video playback. Default value: ENABLE Possible values = ENABLE, DISABLE
multimonitorsupport	<String>	Read-write	Enable/Disable Multiple Monitor Support for Remote

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Desktop Connection (RDC). Default value: ENABLE Possible values = ENABLE, DISABLE
rdpcookievalidity	<Integer>	Read-write	RDP cookie validity period. RDP cookie validity time is applicable for new connection and also for any re-connection that might happen, mostly due to network disruption or during fail-over. Default value: 60 Minimum value = 1 Maximum value = 86400
addusernameinrdpfile	<String>	Read-write	Add username in rdp file. Default value: NO Possible values = YES, NO
rdpfilename	<String>	Read-write	RDP file name to be sent to End User. Minimum length = 1
rdphost	<String>	Read-write	Fully-qualified domain name (FQDN) of the RDP Listener.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum length = 252
rdplistener	<String>	Read-write	IP address (or) Fully-qualified domain name(FQDN) of the RDP Listener with the port in the format IP:Port (or) FQDN:Port. Maximum length = 255
rdpcustomparams	<String>	Read-write	Option for RDP custom parameters settings (if any). Custom params needs to be separated by ';'. Default value: 0 Minimum length = 1
psk	<String>	Read-write	Pre shared key value. Default value: 0
randomizerdpfilename	<String>	Read-write	Will generate unique filename everytime rdp file is downloaded by appending output of time() function in the format <rdpfileName>_<time>.rdp. This tries to avoid the pop-up for replacement of existing rdp file during each rdp connection launch,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			hence providing better end-user experience. Default value: NO Possible values = YES, NO
rdplinkattribute	<String>	Read-write	Citrix Gateway allows the configuration of rdpLinkAttribute parameter which can be used to fetch a list of RDP servers(IP/FQDN) that a user can access, from an Authentication server attribute(Example: LDAP, SAML). Based on the list received, the RDP links will be generated and displayed to the user. Note: The Attribute mentioned in the rdpLinkAttribute should be fetched through corresponding authentication method.
rdpvalidateclientip	<String>	Read-write	This setting determines whether RDC launch is initiated by the valid client IP.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: DISABLE Possible values = ENABLE, DISABLE
rdpurlmaxlencheck	<String>	Read-write	This setting determines whether the RDP URL max length check is enforced during RDP file generation. Default value: DISABLE Possible values = ENABLE, DISABLE
rdpurlmaxlen	<Integer>	Read-write	Indicates the permissible max length of the RDP URL. Set to 256 by default. Default value: 256 Minimum value = 32 Maximum value = 2048
builtin	<String[]>	Read-only	Indicates that a variable is a built-in (SYSTEM INTERNAL) type. Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
feature	<String>	Read-only	The feature to be checked while applying this config.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT
- DELETE

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/rdpclientprofile **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"rdpclientprofile":{

<b>"name":<String_value>,

</b>"rdpurloverride":<String_value>,

"redirectclipboard":<String_value>,

"redirectdrives":<String_value>,

"redirectprinters":<String_value>,

"redirectcomports":<String_value>,

"redirectpnpdevices":<String_value>,

"keyboardhook":<String_value>,

"audiocapturemode":<String_value>,

"videoplaybackmode":<String_value>,

"multimonitorsupport":<String_value>,
```

```
"rdpcookievalidity":<Integer_value>,

"addusernameinrdpfile":<String_value>,

"rdpfilename":<String_value>,

"rdphost":<String_value>,

"rdplistener":<String_value>,

"rdpcustomparams":<String_value>,

"psk":<String_value>,

"randomizerdpfilename":<String_value>,

"rdplinkattribute":<String_value>,

"rdpvalidateclientip":<String_value>,

"rdpurlmaxlencheck":<String_value>,

"rdpurlmaxlen":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/rdpclientprofile **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"rdpclientprofile":{

<b>"name":<String_value>,

</b>"rdpurloverride":<String_value>,

"redirectclipboard":<String_value>,

"redirectdrives":<String_value>,

"redirectprinters":<String_value>,

"redirectcomports":<String_value>,

"redirectpnpdevices":<String_value>,

"keyboardhook":<String_value>,

"audiocapturemode":<String_value>,

"videoplaybackmode":<String_value>,

"multimonitorsupport":<String_value>,

"rdpcookievalidity":<Integer_value>,

"addusernameinrdpfile":<String_value>,

"rdpfilename":<String_value>,

"rdphost":<String_value>,

"rdplistener":<String_value>,

"rdpcustomparams":<String_value>,

"psk":<String_value>,

"randomizerdpfilename":<String_value>,

"rdplinkattribute":<String_value>,

"rdpvalidateclientip":<String_value>,
```

```
"rdpurlmaxlencheck":<String_value>,

"rdpurlmaxlen":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/rdpclientprofile? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"rdpclientprofile":{

<b>"name":<String_value>,

</b>"rdpurloverride":true,

"redirectclipboard":true,

"redirectdrives":true,

"redirectprinters":true,

"redirectcomports":true,

"redirectpnpdevices":true,

"keyboardhook":true,
```

```
"audiocapturemode":true,

"videoplaybackmode":true,

"multimonitorsupport":true,

"rdpcookievalidity":true,

"addusernameinrdpfile":true,

"rdpfilename":true,

"rdphost":true,

"rdplistener":true,

"rdpcustomparams":true,

"psk":true,

"randomizerdpfilename":true,

"rdplinkattribute":true,

"rdpvalidateclientip":true,

"rdpurlmaxlencheck":true,

"rdpurlmaxlen":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/rdpclientprofile/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/rdpclientprofile **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/rdpclientprofile? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/rdpclientprofile? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of rdpclientprofile resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/rdpclientprofile? **view=summary**

Use this query-parameter to get the summary output of rdpclientprofile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/rdpclientprofile? **pagesize=#no;pageno=#no**

Use this query-parameter to get the rdpclientprofile resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "rdpclientprofile": [ {

"name":<String_value>,

"rdpurloverride":<String_value>,

"redirectclipboard":<String_value>,

"redirectdrives":<String_value>,

"redirectprinters":<String_value>,

"redirectcomports":<String_value>,

"redirectpnpdevices":<String_value>,

"keyboardhook":<String_value>,

"audiocapturemode":<String_value>,

"videoplaybackmode":<String_value>,

"multimonitorsupport":<String_value>,

"rdpcookievalidity":<Integer_value>,

"addusernameinrdpfile":<String_value>,

"rdpfilename":<String_value>,

"rdphost":<String_value>,

"rdplistener":<String_value>,

"rdpcustomparams":<String_value>,

"psk":<String_value>,
```

```
"randomizerdpfilename":<String_value>,

"rdplinkattribute":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"rdpvalidateclientip":<String_value>,

"rdpurlmaxlencheck":<String_value>,

"rdpurlmaxlen":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/rdpclientprofile/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/rdpclientprofile/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/rdpclientprofile/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of rdpclientprofile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "rdpclientprofile": [ {

"name":<String_value>,

"rdpurloverride":<String_value>,

"redirectclipboard":<String_value>,

"redirectdrives":<String_value>,

"redirectprinters":<String_value>,

"redirectcomports":<String_value>,

"redirectpnpdevices":<String_value>,

"keyboardhook":<String_value>,

"audiocapturemode":<String_value>,

"videoplaybackmode":<String_value>,

"multimonitorsupport":<String_value>,

"rdpcookievalidity":<Integer_value>,

"addusernameinrdpfile":<String_value>,

"rdpfilename":<String_value>,

"rdphost":<String_value>,

"rdplistener":<String_value>,
```

```
"rdpcustomparams":<String_value>,

"psk":<String_value>,

"randomizerdpfilename":<String_value>,

"rdplinkattribute":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"rdpvalidateclientip":<String_value>,

"rdpurlmaxlencheck":<String_value>,

"rdpurlmaxlen":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/rdpclientprofile? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "rdpclientprofile": [ { "__count": "#no"} ] }
```

rdpconnections

Configuration for active rdp connections resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
username	<String>	Read-write	User name for which to display connections. Minimum length = 1
all	<Boolean>	Read-write	Terminate all active rdpconnections.
endpointip	<String>	Read-only	The client IP address.
endpointport	<Integer>	Read-only	The client port. Range 1 - 65535 * in CLI is represented as 65535 in NITRO API
targetip	<String>	Read-only	The Server IP address.
targetport	<Integer>	Read-only	The server port. Range 1 - 65535 * in CLI is represented as 65535 in NITRO API

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
peid	<Integer>	Read-only	Core id of the session owner.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET (ALL)
- COUNT
- KILL

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

KILL

URL: http:// <netscaler-ip-address> /nitro/v1/config/rdpconnections? **action=kill HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"rdpconnections":{

"username":<String_value>,

"all":<Boolean_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/rdpconnections **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/rdpconnections? **args=username: <String_value>**

Use this query-parameter to get rdpconnections resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/config/rdpconnections? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/rdpconnections? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of rdpconnections resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/rdpconnections? **view=summary**

Use this query-parameter to get the summary output of rdpconnections resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/rdpconnections? **pagesize=#no;pageno=#no**

Use this query-parameter to get the rdpconnections resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "rdpconnections": [ {

username:<String_value>"endpointip":<String_value>,

"endpointport":<Integer_value>,

"targetip":<String_value>,

"targetport":<Integer_value>,

"peid":<Integer_value>,
```

```
"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/rdpconnections? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "rdpconnections": [ { "__count": "#no"} ] }
```

rdpserverprofile

Configuration for RDP serverprofile resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	The name of the rdp server profile. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum length = 32
rdpip	<String>	Read-write	IPv4 or IPv6 address of RDP listener. This terminates client RDP connections. Minimum length = 1
rdpport	<Integer>	Read-write	TCP port on which the RDP connection is established. Default value: 3389 Minimum value = 1 Maximum value = 65535
psk	<String>	Read-write	Pre shared key value.
rdpredirection	<String>	Read-write	Enable/Disable RDP redirection support. This needs to be enabled in presence of connection broker or session directory with IP cookie(msts cookie) based redirection support. Default value: DISABLE Possible values = ENABLE, DISABLE
builtin	<String[]>	Read-only	Indicates that a variable is a built-in (SYSTEM INTERNAL) type.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL
feature	<String>	Read-only	The feature to be checked while applying this config.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT
- DELETE

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of

creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/rdpserverprofile **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"rdpserverprofile":{

<b>"name":<String_value>,

</b>"rdpip":<String_value>,

"rdpport":<Integer_value>,

<b>"psk":<String_value>,

</b>"rdpredirection":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/rdpserverprofile **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"rdpserverprofile":{

<b>"name":<String_value>,

</b>"rdpip":<String_value>,

"rdpport":<Integer_value>,

"psk":<String_value>,

"rdpredirection":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/rdpserverprofile? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"rdpserverprofile":{

<b>"name":<String_value>,

</b>"rdpip":true,

"rdpport":true,

"psk":true,

"rdpredirection":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/rdpserverprofile/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/rdpserverprofile **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/rdpserverprofile? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/rdpserverprofile? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of rdpserverprofile resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/rdpserverprofile? **view=summary**

Use this query-parameter to get the summary output of rdpserverprofile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/rdpserverprofile? **pagesize=#no;pageno=#no**

Use this query-parameter to get the rdpserverprofile resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "rdpserverprofile": [ {

"name":<String_value>,

"rdpip":<String_value>,

"rdpport":<Integer_value>,
```

```
"psk":<String_value>,

"rdpredirection":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/rdpserverprofile/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/rdpserverprofile/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/rdpserverprofile/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of rdpserverprofile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "rdpserverprofile": [ {

"name":<String_value>,

"rdpip":<String_value>,

"rdpport":<Integer_value>,

"psk":<String_value>,

"rdpredirection":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/rdpserverprofile? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "rdpserverprofile": [ { "__count": "#no"} ] }
```

reputation

Reputation

Reputation services configuration.

NAME	DESCRIPTION
reputationsettings	Configuration for Reputation service settings

reputationsettings

Configuration for Reputation service settings resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
proxyserver	<String>	Read-write	Proxy server IP to get Reputation data. Minimum length = 1
proxyport	<Integer>	Read-write	Proxy server port.
proxyusername	<String>	Read-write	Proxy Username. Minimum length = 1
proxypassword	<String>	Read-write	Password with which user logs on. Minimum length = 1
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- UPDATE
- UNSET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/reputationsettings **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"reputationsettings":{

"proxyserver":<String_value>,

"proxyport":<Integer_value>,

"proxyusername":<String_value>,

"proxypassword":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/reputationsettings? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"reputationsettings":{

"proxyserver":true,

"proxyport":true,

"proxyusername":true,

"proxypassword":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/reputationsettings **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "reputationsettings": [ {

"proxyserver":<String_value>,

"proxyport":<Integer_value>,

"proxyusername":<String_value>,

"proxypassword":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

responder

Responder

Responder configuration.

NAME	DESCRIPTION
responderaction	Configuration for responder action
responderglobal_binding	Binding object showing the resources that can be bound to responderglobal
responderglobal_responderpolicy_binding	Binding object showing the responderpolicy that can be bound to responderglobal
responderhtmlpage	Configuration for Responder HTML page
responderparam	Configuration for responser parameter
responderpolicy	Configuration for responder policy
responderpolicy_binding	Binding object showing the resources that can be bound to responderpolicy
responderpolicy_crvserver_binding	Binding object showing the crvserver that can be bound to responderpolicy
responderpolicy_csvserver_binding	Binding object showing the csvserver that can be bound to responderpolicy
responderpolicy_lbvserver_binding	Binding object showing the lbvserver that can be bound to responderpolicy

NAME	DESCRIPTION
responderpolicy_responderglobal_binding	Binding object showing the responderglobal that can be bound to responderpolicy
responderpolicy_responderpolicylabel_binding	Binding object showing the responderpolicylabel that can be bound to responderpolicy
responderpolicy_vpnvserver_binding	Binding object showing the vpnvserver that can be bound to responderpolicy
responderpolicylabel	Configuration for responder policy label
responderpolicylabel_binding	Binding object showing the resources that can be bound to responderpolicylabel
responderpolicylabel_policybinding_binding	Binding object showing the policybinding that can be bound to responderpolicylabel
responderpolicylabel_responderpolicy_binding	Binding object showing the responderpolicy that can be bound to responderpolicylabel

responderaction

Configuration for responder action resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the responder action. Must begin with a letter, number, or the underscore character

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			(_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Can be changed after the responder policy is added. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my responder action" or 'my responder action').
type	<String>	Read-write	Type of responder action. Available settings function as follows: * respondwith <target> - Respond to the request with the expression specified as the target.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			* respondwithhtmlpage - Respond to the request with the uploaded HTML page object specified as the target. * redirect - Redirect the request to the URL specified as the target. * sqlresponse_ok - Send an SQL OK response. * sqlresponse_error - Send an SQL ERROR response. Possible values = noop, respondwith, redirect, respondwithhtmlpage, sqlresponse_ok, sqlresponse_error
target	<String>	Read-write	Expression specifying what to respond with. Typically a URL for redirect policies or a default-syntax expression. In addition to Citrix ADC default-syntax expressions that

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			refer to information in the request, a stringbuilder expression can contain text and HTML, and simple escape codes that define new lines and paragraphs. Enclose each stringbuilder expression element (either a Citrix ADC default-syntax expression or a string) in double quotation marks. Use the plus (+) character to join the elements. Examples: 1) Respondwith expression that sends an HTTP 1.1 200 OK response: "HTTP/1.1 200 OK\r\n\r\n" 2) Redirect expression that redirects user to the specified web host and appends the request URL to the redirect.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			"http://backupsite2.com" + HTTP.REQ.URL 3) Respondwith expression that sends an HTTP 1.1 404 Not Found response with the request URL included in the response: "HTTP/1.1 404 Not Found\r\n\r\n"+ "HTTP.REQ.URL.HTTP_URL_SAFE" + "does not exist on the web server." The following requirement applies only to the Citrix ADC CLI: Enclose the entire expression in single quotation marks. (Citrix ADC expression elements should be included inside the single quotation marks for the entire expression, but do not need to be

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			enclosed in double quotation marks.).
htmlpage	<String>	Read-write	For respondwithhtmlpage policies, name of the HTML page object to use as the response. You must first import the page object. Minimum length = 1
bypasssafetycheck	<String>	Read-write	Bypass the safety check, allowing potentially unsafe expressions. An unsafe expression in a response is one that contains references to request elements that might not be present in all requests. If a response refers to a missing request element, an empty string is used instead. Default value: NO Possible values = YES, NO
comment	<String>	Read-write	Comment. Any type of information about this responder action.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
responsestatuscode	<Integer>	Read-write	HTTP response status code, for example 200, 302, 404, etc. The default value for the redirect action type is 302 and for respondwithhtmlpage is 200. Minimum value = 100 Maximum value = 599
reasonphrase	<String>	Read-write	Expression specifying the reason phrase of the HTTP response. The reason phrase may be a string literal with quotes or a PI expression. For example: "Invalid URL: " + HTTP.REQ.URL. Minimum length = 1
headers	<String[]>	Read-write	One or more headers to insert into the HTTP response. Each header is specified as "name(expr)", where expr is an expression that is evaluated at runtime to provide the value for the named header. You can configure a

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			maximum of eight headers for a responder action.
newname	<String>	Read-write	New name for the responder action. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space ( ), at (@), equals (=), colon (:), and underscore characters. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my responder action" or my responder action'). Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
hits	<Integer>	Read-only	The number of times the action has been taken.
referencecount	<Integer>	Read-only	The number of references to the action.
undefhits	<Integer>	Read-only	The number of times the action resulted in UNDEF.
builtin	<String[]>	Read-only	Flag to determine whether responder action is built-in or not. Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL
feature	<String>	Read-only	The feature to be checked while applying this config.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)

- GET
- COUNT
- RENAME

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/responderaction **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"responderaction":{

<b>"name":<String_value>,

</b><b>"type":<String_value>,

</b>"target":<String_value>,

"htmlpage":<String_value>,

"bypasssafetycheck":<String_value>,

"comment":<String_value>,

"responsestatuscode":<Integer_value>,

"reasonphrase":<String_value>,

"headers":<String[]_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/responderaction/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/responderaction **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"responderaction":{

<b>"name":<String_value>,

</b>"target":<String_value>,

"bypasssafetycheck":<String_value>,

"htmlpage":<String_value>,

"responsestatuscode":<Integer_value>,

"reasonphrase":<String_value>,

"comment":<String_value>,

"headers":<String[]_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/responderaction? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"responderaction":{

<b>"name":<String_value>,

</b>"responsestatuscode":true,

"reasonphrase":true,

"comment":true,

"headers":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

RENAME

URL: http:// <netscaler-ip-address> /nitro/v1/config/responderaction? **action=rename HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"responderaction":{

<b>"name":<String_value>,

</b><b>"newname":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/responderaction **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/responderaction? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/responderaction? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of responderaction resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/responderaction? **view=summary**

Use this query-parameter to get the summary output of responderaction resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/responderaction? **pagesize=#no;pageno=#no**

Use this query-parameter to get the responderaction resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "responderaction": [ {

"name":<String_value>,

"type":<String_value>,

"target":<String_value>,

"htmlpage":<String_value>,

"bypasssafetycheck":<String_value>,

"hits":<Integer_value>,

"referencecount":<Integer_value>,

"undefhits":<Integer_value>,

"comment":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"responsestatuscode":<Integer_value>,

"reasonphrase":<String_value>,

"headers":<String[]_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/responderaction/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/responderaction/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/responderaction/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of responderaction resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "responderaction": [ {

"name":<String_value>,

"type":<String_value>,

"target":<String_value>,

"htmlpage":<String_value>,
```

```
"bypasssafetycheck":<String_value>,

"hits":<Integer_value>,

"referencecount":<Integer_value>,

"undefhits":<Integer_value>,

"comment":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"responsestatuscode":<Integer_value>,

"reasonphrase":<String_value>,

"headers":<String[]_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/responderaction? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "responderaction": [ { "__count": "#no"} ] }
```

responderglobal_binding

Binding object which returns the resources bound to responderglobal.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
responderglobal_responderpolicy_binding	<responderglobal_responderpolicy_binding[]>	Read-write	responderpolicy that can be bound to responderglobal.

Operations

(click to see Properties)

- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/responderglobal_binding

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "responderglobal_binding": [ {

"responderglobal_responderpolicy_binding":<responderglobal_responderpolicy
_binding[]_value>

}]}
```

responderglobal_responderpolicy_binding

Binding object showing the responderpolicy that can be bound to responderglobal.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
labeltype	<String>	Read-write	Type of invocation, Available settings function as follows: * vserver - Forward the request to the specified virtual server. * policylabel - Invoke the specified policy label. Possible values = vserver, policylabel
priority	<Integer>	Read-write	Specifies the priority of the policy.
labelname	<String>	Read-write	Name of the policy label to invoke. If the current policy evaluates to TRUE, the invoke parameter is set, and Label Type is policylabel.
type	<String>	Read-write	Specifies the bind point whose policies you want to display. Available settings function as follows: * REQ_OVERRIDE - Request override. Binds the policy to the priority request queue. * REQ_DEFAULT -

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Binds the policy to the default request queue. * OTHERTCP_REQ_OVERRIDE - Binds the policy to the non-HTTP TCP priority request queue. * OTHERTCP_REQ_DEFAULT - Binds the policy to the non-HTTP TCP default request queue.. * SIPUDP_REQ_OVERRIDE - Binds the policy to the SIP UDP priority response queue.. * SIPUDP_REQ_DEFAULT - Binds the policy to the SIP UDP default response queue. * RADIUS_REQ_OVERRIDE - Binds the policy to the RADIUS priority response queue.. * RADIUS_REQ_DEFAULT - Binds the policy to the RADIUS default response queue. * MSSQL_REQ_OVERRIDE - Binds the policy to the Microsoft SQL priority response queue.. * MSSQL_REQ_DEFAULT - Binds the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			policy to the Microsoft SQL default response queue. * MYSQL_REQ_OVERRIDE - Binds the policy to the MySQL priority response queue. * MYSQL_REQ_DEFAULT - Binds the policy to the MySQL default response queue. * HTTPQUIC_REQ_OVERRIDE - Binds the policy to the HTTP_QUIC override response queue. * HTTPQUIC_REQ_DEFAULT - Binds the policy to the HTTP_QUIC default response queue. * UDP_REQ_OVERRIDE - Binds the policy to the UDP request override queue. * UDP_REQ_DEFAULT - Binds the policy to the UDP request default queue. Possible values = REQ_OVERRIDE, REQ_DEFAULT, OVERRIDE, DEFAULT, OTHERTCP_REQ_OVERRIDE,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			OTHERTCP_REQ_DEFAULT, SIPUDP_REQ_OVERRIDE, SIPUDP_REQ_DEFAULT, SIPTCP_REQ_OVERRIDE, SIPTCP_REQ_DEFAULT, MSSQL_REQ_OVERRIDE, MSSQL_REQ_DEFAULT, MYSQL_REQ_OVERRIDE, MYSQL_REQ_DEFAULT, NAT_REQ_OVERRIDE, NAT_REQ_DEFAULT, DIAMETER_REQ_OVERRIDE, DIAMETER_REQ_DEFAULT, RADIUS_REQ_OVERRIDE, RADIUS_REQ_DEFAULT, DNS_REQ_OVERRIDE, DNS_REQ_DEFAULT, MQTT_REQ_OVERRIDE,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			MQTT_REQ_DEFAULT, MQTT_JUMBO_REQ_OVERRIDE, MQTT_JUMBO_REQ_DEFAULT, QUIC_OVERRIDE, QUIC_DEFAULT, HTTPQUIC_REQ_OVERRIDE, HTTPQUIC_REQ_DEFAULT, UDP_REQ_OVERRIDE, UDP_REQ_DEFAULT
gotopriorityexpression	<String>	Read-write	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
invoke	<Boolean>	Read-write	If the current policy evaluates to TRUE, terminate evaluation of policies bound to the current policy label, and then forward the request to the specified virtual server or evaluate the specified policy label.
globalbindtype	<String>	Read-write	.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: SYSTEM_GLOBAL Possible values = SYSTEM_GLOBAL, VPN_GLOBAL, RNAT_GLOBAL, APPFW_GLOBAL, TM_GLOBAL
policyname	<String>	Read-write	Name of the responder policy.
flowtype	<Integer>	Read-only	flowtype of the bound responder policy.
numpol	<Integer>	Read-only	number of polices bound to label.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/responderglobal_responderpolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"responderglobal_responderpolicy_binding":{

<b>"policyname":<String_value>,

</b><b>"priority":<Integer_value>,

</b>"gotopriorityexpression":<String_value>,

"type":<String_value>,
```

```
"invoke":<Boolean_value>,

"labeltype":<String_value>,

"labelname":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/responderglobal_responderpolicy_binding **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/responderglobal_responderpolicy_binding? **args= policyname:<String_value>, type: <String_value> ,priority: <Integer_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/responderglobal_responderpolicy_binding **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/responderglobal_responderpolicy_binding? **args=type: <String_value>**

Use this query-parameter to get responderglobal_responderpolicy_binding resources based on additional properties.

filter http:// <netscaler-ip-address> /nitro/v1/config/responderglobal_responderpolicy_binding? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of responderglobal_responderpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ responderglobal_responderpolicy_binding? **pagesize=#no;pageno=#no**

Use this query-parameter to get the responderglobal_responderpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "responderglobal_responderpolicy_binding": [ {

"labeltype":<String_value>,

"priority":<Integer_value>,

"labelname":<String_value>,

"type":<String_value>,

"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>,

"globalbindtype":<String_value>,
```

```
"policyname":<String_value>,

"flowtype":<Integer_value>,

"numpol":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/responderglobal_responderpolicy_binding?**count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "responderglobal_responderpolicy_binding": [ { "__count": "#no"} ] }
```

responderhtmlpage

Configuration for Responder HTML page resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
src	<String>	Read-write	Local path or URL (protocol, host, path, and file name) for the file from which to retrieve the imported HTML page. NOTE: The import fails if the object to be imported is on an HTTPS server that requires client certificate authentication for access. Minimum length = 1 Maximum length = 2047
name	<String>	Read-write	Name to assign to the HTML page object on the Citrix ADC. Minimum length = 1 Maximum length = 31
comment	<String>	Read-write	Any comments to preserve information about the HTML page object. Maximum length = 128
overwrite	<Boolean>	Read-write	Overwrites the existing file.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
cacertfile	<String>	Read-write	CA certificate file name which will be used to verify the peer's certificate. The certificate should be imported using "import ssl certfile" CLI command or equivalent in API or GUI. If certificate name is not configured, then default root CA certificates are used for peer's certificate verification.
response	<String>	Read-only	.
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- IMPORT
- DELETE
- CHANGE
- GET (ALL)
- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

IMPORT

URL: http:// <netscaler-ip-address> /nitro/v1/config/responderhtmlpage? **action=Import HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"responderhtmlpage":{

"src":<String_value>,

<b>"name":<String_value>,

</b>"comment":<String_value>,

"overwrite":<Boolean_value>,

"cacertfile":<String_value>
```

```
}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/responderhtmlpage/ name_value<String>
HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

CHANGE

URL: http:// <netscaler-ip-address> /nitro/v1/config/responderhtmlpage? **action=update HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"responderhtmlpage":{

<b>"name":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/responderhtmlpage **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "responderhtmlpage": [ {

"name":<String_value>,

"response":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/responderhtmlpage/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/responderhtmlpage/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/responderhtmlpage/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of responderhtmlpage resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "responderhtmlpage": [ {

"name":<String_value>,

"response":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

responderparam

Configuration for responser parameter resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
undefaction	<String>	Read-write	Action to perform when policy evaluation creates an UNDEF condition. Available settings function as follows: * NOOP - Send the request to the protected server. * RESET - Reset the request and notify the user's browser, so that the user can resend the request. * DROP - Drop the request without sending a response to the user. Default value: "NOOP"
timeout	<Integer>	Read-write	Maximum time in milliseconds to allow for processing all the policies and their selected actions without interruption. If the timeout is reached then the evaluation causes an UNDEF to be raised and no further processing is performed.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: 3900 Minimum value = 1 Maximum value = 5000
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- UPDATE
- UNSET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/responderparam **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"responderparam":{

"undefaction":<String_value>,

"timeout":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/responderparam? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"responderparam":{

"undefaction":true,

"timeout":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/responderparam **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "responderparam": [ {

"undefaction":<String_value>,

"timeout":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

responderpolicy

Configuration for responder policy resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the responder policy. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Can be changed after the responder policy is added. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			"my responder policy" or 'my responder policy').
rule	<String>	Read-write	Expression that the policy uses to determine whether to respond to the specified request.
action	<String>	Read-write	Name of the responder action to perform if the request matches this responder policy. There are also some built-in actions which can be used. These are: * NOOP - Send the request to the protected server instead of responding to it. * RESET - Reset the client connection by closing it. The client program, such as a browser, will handle this and may inform the user. The client may then resend the request if desired.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			* DROP - Drop the request without sending a response to the user.
undefaction	<String>	Read-write	Action to perform if the result of policy evaluation is undefined (UNDEF). An UNDEF event indicates an internal error condition. Only the above built-in actions can be used.
comment	<String>	Read-write	Any type of information about this responder policy.
logaction	<String>	Read-write	Name of the messagelog action to use for requests that match this policy.
appflowaction	<String>	Read-write	AppFlow action to invoke for requests that match this policy.
newname	<String>	Read-write	New name for the responder policy. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space ( ), at (@), equals (=), colon (:), and

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			underscore characters. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my responder policy" or 'my responder policy'). Minimum length = 1
hits	<Integer>	Read-only	Number of hits.
undefhits	<Integer>	Read-only	Number of policy UNDEF hits.
builtin	<String[]>	Read-only	Flag to determine if responder policy is built-in or not. Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL
feature	<String>	Read-only	The feature to be checked while applying this config.
_nextgenapiresource	<String>	Read-only	.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT
- RENAME

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/responderpolicy **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"responderpolicy":{

<b>"name":<String_value>,

</b><b>"rule":<String_value>,

</b><b>"action":<String_value>,

</b>"undefaction":<String_value>,

"comment":<String_value>,

"logaction":<String_value>,

"appflowaction":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/responderpolicy/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/responderpolicy **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"responderpolicy":{

<b>"name":<String_value>,

</b>"rule":<String_value>,

"action":<String_value>,

"undefaction":<String_value>,

"comment":<String_value>,

"logaction":<String_value>,

"appflowaction":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/responderpolicy? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"responderpolicy":{

<b>"name":<String_value>,

</b>"undefaction":true,

"comment":true,

"logaction":true,

"appflowaction":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

RENAME

URL: http:// <netscaler-ip-address> /nitro/v1/config/responderpolicy? **action=rename HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"responderpolicy":{

<b>"name":<String_value>,

</b><b>"newname":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/responderpolicy **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/responderpolicy? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/responderpolicy? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of responderpolicy resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/responderpolicy? **view=summary**

Use this query-parameter to get the summary output of responderpolicy resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/responderpolicy? **pagesize=#no;pageno=#no**

Use this query-parameter to get the responderpolicy resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "responderpolicy": [ {

"name":<String_value>,

"rule":<String_value>,

"action":<String_value>,

"undefaction":<String_value>,

"hits":<Integer_value>,

"undefhits":<Integer_value>,

"comment":<String_value>,

"logaction":<String_value>,

"appflowaction":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/responderpolicy/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/responderpolicy/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/responderpolicy/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of responderpolicy resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "responderpolicy": [ {

"name":<String_value>,

"rule":<String_value>,

"action":<String_value>,

"undefaction":<String_value>,
```

```
"hits":<Integer_value>,

"undefhits":<Integer_value>,

"comment":<String_value>,

"logaction":<String_value>,

"appflowaction":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/responderpolicy? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "responderpolicy": [ { "__count": "#no"} ] }
```

responderpolicy_binding

Binding object which returns the resources bound to responderpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the responder policy for which to display settings.
responderpolicy_responderglobal_binding	<responderpolicy_responderglobal_binding[]>	Read-only	responderglobal that can be bound to responderpolicy.
responderpolicy_lbvserver_binding	<responderpolicy_lbvserver_binding[]>	Read-only	lbvserver that can be bound to responderpolicy.
responderpolicy_responderpolicylabel_binding	<responderpolicy_responderpolicylabel_binding[]>	Read-only	responderpolicylabel that can be bound to responderpolicy.
responderpolicy_crvserver_binding	<responderpolicy_crvserver_binding[]>	Read-only	crvserver that can be bound to responderpolicy.
responderpolicy_vpnvserver_binding	<responderpolicy_vpnvserver_binding[]>	Read-only	vpnvserver that can be bound to responderpolicy.
responderpolicy_csvserver_binding	<responderpolicy_csvserver_binding[]>	Read-only	csvserver that can be bound to responderpolicy.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/responderpolicy_binding/ name_value<String>
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "responderpolicy_binding": [ {

"name":<String_value>,

"responderpolicy_responderpolicylabel_binding":<responderpolicy_responderp
olicylabel_binding[]_value>,

"responderpolicy_crvserver_binding":<responderpolicy_crvserver_binding[]_v
alue>,

"responderpolicy_lbvserver_binding":<responderpolicy_lbvserver_binding[]_v
alue>,

"responderpolicy_responderglobal_binding":<responderpolicy_responderglobal
_binding[]_value>,

"responderpolicy_csvserver_binding":<responderpolicy_csvserver_binding[]_v
alue>,

"responderpolicy_vpnvserver_binding":<responderpolicy_vpnvserver_binding[]
_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/responderpolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/responderpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "responderpolicy_binding": [ {

"name":<String_value>,

"responderpolicy_responderpolicylabel_binding":<responderpolicy_responderp
olicylabel_binding[]_value>,

"responderpolicy_crvserver_binding":<responderpolicy_crvserver_binding[]_v
alue>,

"responderpolicy_lbvserver_binding":<responderpolicy_lbvserver_binding[]_v
alue>,

"responderpolicy_responderglobal_binding":<responderpolicy_responderglobal
_binding[]_value>,

"responderpolicy_csvserver_binding":<responderpolicy_csvserver_binding[]_v
alue>,

"responderpolicy_vpnvserver_binding":<responderpolicy_vpnvserver_binding[]
_value>

}]}
```

responderpolicy_crvserver_binding

Binding object showing the crvserver that can be bound to responderpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
boundto	<String>	Read-write	Location where policy is bound.
name	<String>	Read-write	Name of the responder policy for which to display settings.
priority	<Integer>	Read-only	Specifies the priority of the policy.
labeltype	<String>	Read-only	Type of policy label invocation. Possible values = reqvserver, resvserver, policylabel
activepolicy	<Integer>	Read-only	Indicates whether policy is bound or not.
gotopriorityexpression	<String>	Read-only	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
labelname	<String>	Read-only	Name of the label to invoke if the current policy rule evaluates to TRUE.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/responderpolicy_crvserver_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ responderpolicy_crvserver_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of responderpolicy_crvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/responderpolicy_crvserver_binding/name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the responderpolicy_crvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "responderpolicy_crvserver_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"priority":<Integer_value>,

"labeltype":<String_value>,

"activepolicy":<Integer_value>,

"gotopriorityexpression":<String_value>,

"labelname":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/responderpolicy_crvserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/responderpolicy_crvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "responderpolicy_crvserver_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"priority":<Integer_value>,

"labeltype":<String_value>,

"activepolicy":<Integer_value>,

"gotopriorityexpression":<String_value>,
```

```
"labelname":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/responderpolicy_crvserver_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"responderpolicy_crvserver_binding": [ { "__count": "#no"} ] }
```

responderpolicy_csvserver_binding

Binding object showing the csvserver that can be bound to responderpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
boundto	<String>	Read-write	Location where policy is bound.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the responder policy for which to display settings.
labeltype	<String>	Read-only	Type of policy label invocation. Possible values = reqvserver, resvserver, policylabel
priority	<Integer>	Read-only	Specifies the priority of the policy.
labelname	<String>	Read-only	Name of the label to invoke if the current policy rule evaluates to TRUE.
gotopriorityexpression	<String>	Read-only	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
activepolicy	<Integer>	Read-only	Indicates whether policy is bound or not.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)

- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/responderpolicy_csvserver_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ responderpolicy_csvserver_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of responderpolicy_csvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/responderpolicy_csvserver_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the responderpolicy_csvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "responderpolicy_csvserver_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"labelname":<String_value>,

"gotopriorityexpression":<String_value>,

"activepolicy":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/responderpolicy_csvserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/responderpolicy_csvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "responderpolicy_csvserver_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"labelname":<String_value>,

"gotopriorityexpression":<String_value>,

"activepolicy":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/responderpolicy_csvserver_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"responderpolicy_csvserver_binding": [ { "__count": "#no"} ] }
```

responderpolicy_lbvserver_binding

Binding object showing the lbvserver that can be bound to responderpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the responder policy for which to display settings.
boundto	<String>	Read-write	Location where policy is bound.
priority	<Integer>	Read-only	Specifies the priority of the policy.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
labeltype	<String>	Read-only	Type of policy label invocation. Possible values = reqvserver, resvserver, policylabel
activepolicy	<Integer>	Read-only	Indicates whether policy is bound or not.
gotopriorityexpression	<String>	Read-only	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
labelname	<String>	Read-only	Name of the label to invoke if the current policy rule evaluates to TRUE.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/responderpolicy_lbvserver_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ responderpolicy_lbvserver_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of responderpolicy_lbvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/responderpolicy_lbvserver_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the responderpolicy_lbvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "responderpolicy_lbvserver_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"priority":<Integer_value>,

"labeltype":<String_value>,

"activepolicy":<Integer_value>,

"gotopriorityexpression":<String_value>,

"labelname":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/responderpolicy_lbvserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/responderpolicy_lbvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "responderpolicy_lbvserver_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"priority":<Integer_value>,

"labeltype":<String_value>,

"activepolicy":<Integer_value>,

"gotopriorityexpression":<String_value>,

"labelname":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/responderpolicy_lbvserver_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"responderpolicy_lbvserver_binding": [ { "__count": "#no"} ] }
```

responderpolicy_responderglobal_binding

Binding object showing the responderglobal that can be bound to responderpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
boundto	<String>	Read-write	Location where policy is bound.
name	<String>	Read-write	Name of the responder policy for which to display settings.
labeltype	<String>	Read-only	Type of policy label invocation. Possible values = reqvserver, resvserver, policylabel
priority	<Integer>	Read-only	Specifies the priority of the policy.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
labelname	<String>	Read-only	Name of the label to invoke if the current policy rule evaluates to TRUE.
gotopriorityexpression	<String>	Read-only	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
activepolicy	<Integer>	Read-only	Indicates whether policy is bound or not.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.
- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of

creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/responderpolicy_responderglobal_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ responderpolicy_responderglobal_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of responderpolicy_responderglobal_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ responderpolicy_responderglobal_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the responderpolicy_responderglobal_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "responderpolicy_responderglobal_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"labelname":<String_value>,

"gotopriorityexpression":<String_value>,

"activepolicy":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/responderpolicy_responderglobal_binding
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/responderpolicy_responderglobal_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "responderpolicy_responderglobal_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"labelname":<String_value>,

"gotopriorityexpression":<String_value>,

"activepolicy":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/responderpolicy_responderglobal_binding/name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"responderpolicy_responderglobal_binding": [ { "__count": "#no"} ] }
```

responderpolicy_responderpolicylabel_binding

Binding object showing the responderpolicylabel that can be bound to responderpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
boundto	<String>	Read-write	Location where policy is bound.
name	<String>	Read-write	Name of the responder policy for which to display settings.
labeltype	<String>	Read-only	Type of policy label invocation. Possible values = reqvserver, resvserver, policylabel
priority	<Integer>	Read-only	Specifies the priority of the policy.
labelname	<String>	Read-only	Name of the label to invoke if the current policy rule evaluates to TRUE.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
gotopriorityexpression	<String>	Read-only	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
activepolicy	<Integer>	Read-only	Indicates whether policy is bound or not.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/responderpolicy_responderpolicylabel_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ responderpolicy_responderpolicylabel_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of responderpolicy_responderpolicylabel_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ responderpolicy_responderpolicylabel_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the responderpolicy_responderpolicylabel_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "responderpolicy_responderpolicylabel_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"labelname":<String_value>,

"gotopriorityexpression":<String_value>,

"activepolicy":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/responderpolicy_responderpolicylabel_binding
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/responderpolicy_responderpolicylabel_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "responderpolicy_responderpolicylabel_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"labelname":<String_value>,

"gotopriorityexpression":<String_value>,

"activepolicy":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/responderpolicy_responderpolicylabel_binding/name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"responderpolicy_responderpolicylabel_binding": [ { "__count": "#no"} ] }
```

responderpolicy_vpnvserver_binding

Binding object showing the vpnvserver that can be bound to responderpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the responder policy for which to display settings.
boundto	<String>	Read-write	Location where policy is bound.
labelname	<String>	Read-only	Name of the label to invoke if the current policy rule evaluates to TRUE.
gotopriorityexpression	<String>	Read-only	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
activepolicy	<Integer>	Read-only	Indicates whether policy is bound or not.
labeltype	<String>	Read-only	Type of policy label invocation. Possible values = reqvserver,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			resvserver, policylabel
priority	<Integer>	Read-only	Specifies the priority of the policy.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/responderpolicy_vpnvserver_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ responderpolicy_vpnvserver_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of responderpolicy_vpnvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/responderpolicy_vpnvserver_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the responderpolicy_vpnvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "responderpolicy_vpnvserver_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"labelname":<String_value>,

"gotopriorityexpression":<String_value>,
```

```
"activepolicy":<Integer_value>,

"labeltype":<String_value>,

"priority":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/responderpolicy_vpnvserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/responderpolicy_vpnvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "responderpolicy_vpnvserver_binding": [ {

"name":<String_value>,

"boundto":<String_value>,
```

```
"labelname":<String_value>,

"gotopriorityexpression":<String_value>,

"activepolicy":<Integer_value>,

"labeltype":<String_value>,

"priority":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/responderpolicy_vpnvserver_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"responderpolicy_vpnvserver_binding": [ { "__count": "#no"} ] }
```

responderpolicylabel

Configuration for responder policy label resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
labelname	<String>	Read-write	Name for the responder policy label. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after the responder policy label is added. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my responder policy label" or my responder policy label').
policylabeltype	<String>	Read-write	Type of responses sent by the policies

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			bound to this policy label. Types are: * HTTP - HTTP responses. * OTHERTCP - NON-HTTP TCP responses. * SIP_UDP - SIP responses. * RADIUS - RADIUS responses. * MYSQL - SQL responses in MySQL format. * MSSQL - SQL responses in Microsoft SQL format. * NAT - NAT response. * MQTT - Trigger policies bind with MQTT type. * MQTT_JUMBO - Trigger policies bind with MQTT Jumbo type. Default value: HTTP Possible values = HTTP, OTHERTCP,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			SIP_UDP, SIP_TCP, MYSQL, MSSQL, NAT, DIAMETER, RADIUS, DNS, MQTT, MQTT_JUMBO, QUIC_BRIDGE, HTTP_QUIC, UDP
comment	<String>	Read-write	Any comments to preserve information about this responder policy label.
newname	<String>	Read-write	New name for the responder policy label. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Minimum length = 1
numpol	<Integer>	Read-only	number of polices bound to label.
hits	<Integer>	Read-only	Number of times policy label was invoked.
priority	<Integer>	Read-only	Specifies the priority of the policy.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
gotopriorityexpression	<String>	Read-only	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
labeltype	<String>	Read-only	Type of policy label to invoke. Available settings function as follows: * vserver - Invoke an unnamed policy label associated with a virtual server. * policylabel - Invoke a user-defined policy label. Possible values = vserver, policylabel
invoke_labelname	<String>	Read-only	* If labelType is policylabel, name of the policy label to invoke. * If labelType is reqvserver or resvserver, name of the virtual server.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET (ALL)
- GET
- COUNT
- RENAME

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/responderpolicylabel **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"responderpolicylabel":{

<b>"labelname":<String_value>,

</b>"policylabeltype":<String_value>,

"comment":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/responderpolicylabel/ labelname_value<String>
HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

RENAME

URL: http:// <netscaler-ip-address> /nitro/v1/config/responderpolicylabel? **action=rename HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"responderpolicylabel":{

<b>"labelname":<String_value>,

</b><b>"newname":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/responderpolicylabel **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/responderpolicylabel? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/responderpolicylabel? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of responderpolicylabel resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/responderpolicylabel? **view=summary**

Use this query-parameter to get the summary output of responderpolicylabel resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/responderpolicylabel? **pagesize=#no;pageno=#no**

Use this query-parameter to get the responderpolicylabel resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "responderpolicylabel": [ {

"labelname":<String_value>,

"policylabeltype":<String_value>,

"numpol":<Integer_value>,

"hits":<Integer_value>,

"priority":<Integer_value>,

"gotopriorityexpression":<String_value>,

"labeltype":<String_value>,

"invoke_labelname":<String_value>,

"comment":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/responderpolicylabel/ labelname_value<String>
Query-parameters: attrs http:// <netscaler-ip-address> /nitro/v1/config/responderpolicylabel/ labelname_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/responderpolicylabel/ labelname_value<String> ? **view=summary**

Use this query-parameter to get the summary output of responderpolicylabel resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "responderpolicylabel": [ {

"labelname":<String_value>,

"policylabeltype":<String_value>,

"numpol":<Integer_value>,

"hits":<Integer_value>,
```

```
"priority":<Integer_value>,

"gotopriorityexpression":<String_value>,

"labeltype":<String_value>,

"invoke_labelname":<String_value>,

"comment":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/responderpolicylabel? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "responderpolicylabel": [ { "__count": "#no"} ] }
```

responderpolicylabel_binding

Binding object which returns the resources bound to responderpolicylabel.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
labelname	<String>	Read-write	Name of the responder policy label.
responderpolicylabel_policybinding_binding	<responderpolicylabel_policybinding_binding[]>	Read-only	policybinding that can be bound to responderpolicylabel.
responderpolicylabel_responderpolicy_binding	<responderpolicylabel_responderpolicy_binding[]>	Read-only	responderpolicy that can be bound to responderpolicylabel.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/responderpolicylabel_binding/ labelname_value<String>

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "responderpolicylabel_binding": [ {

"labelname":<String_value>,

"responderpolicylabel_policybinding_binding":<responderpolicylabel_policybinding_binding[]_value>,

"responderpolicylabel_responderpolicy_binding":<responderpolicylabel_responderpolicy_binding[]_value>
```

```
}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/responderpolicylabel_binding

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters:

bulkbindings

http:// <netscaler-ip-address> /nitro/v1/config/responderpolicylabel_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "responderpolicylabel_binding": [ {

"labelname":<String_value>,

"responderpolicylabel_policybinding_binding":<responderpolicylabel_policyb
```

```
inding_binding[]_value>,

"responderpolicylabel_responderpolicy_binding":<responderpolicylabel_respo
nderpolicy_binding[]_value>

}]}
```

responderpolicylabel_policybinding_binding

Binding object showing the policybinding that can be bound to responderpolicylabel.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
invoke_labelname	<String>	Read-write	* If labelType is policylabel, name of the policy label to invoke. * If labelType is reqvserver or resvserver, name of the virtual server.
invoke	<Boolean>	Read-write	If the current policy evaluates to TRUE, terminate evaluation of policies bound to the current policy label and evaluate the specified policy label.
gotopriorityexpression	<String>	Read-write	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
policyname	<String>	Read-write	Name of the responder policy.
priority	<Integer>	Read-write	Specifies the priority of the policy.
labeltype	<String>	Read-write	Type of policy label to invoke. Available settings function as follows: * vserver - Invoke an unnamed policy label associated with a virtual server. * policylabel - Invoke a user-defined policy label. Possible values = vserver, policylabel
labelname	<String>	Read-write	Name of the responder policy label to which to bind the policy.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/responderpolicylabel_policybinding_binding/ labelname_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ responderpolicylabel_policybinding_binding/ labelname_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of responderpolicylabel_policybinding_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ responderpolicylabel_policybinding_binding/ labelname_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the responderpolicylabel_policybinding_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "responderpolicylabel_policybinding_binding": [ {

"invoke_labelname":<String_value>,

"invoke":<Boolean_value>,

"gotopriorityexpression":<String_value>,

"policyname":<String_value>,

"priority":<Integer_value>,

"labeltype":<String_value>,

"labelname":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/responderpolicylabel_policybinding_binding
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/responderpolicylabel_policybinding_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "responderpolicylabel_policybinding_binding": [ {

"invoke_labelname":<String_value>,

"invoke":<Boolean_value>,

"gotopriorityexpression":<String_value>,

"policyname":<String_value>,

"priority":<Integer_value>,

"labeltype":<String_value>,

"labelname":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/responderpolicylabel_policybinding_binding/labelname_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"responderpolicylabel_policybinding_binding": [ { "__count": "#no"} ] }
```

responderpolicylabel_responderpolicy_binding

Binding object showing the responderpolicy that can be bound to responderpolicylabel.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
gotopriorityexpression	<String>	Read-write	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
invoke	<Boolean>	Read-write	If the current policy evaluates to TRUE, terminate evaluation of policies bound to the current policy label and evaluate the specified policy label.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
policyname	<String>	Read-write	Name of the responder policy.
invoke_labelname	<String>	Read-write	* If labelType is policylabel, name of the policy label to invoke. * If labelType is reqvserver or resvserver, name of the virtual server.
labeltype	<String>	Read-write	Type of policy label to invoke. Available settings function as follows: * vserver - Invoke an unnamed policy label associated with a virtual server. * policylabel - Invoke a user-defined policy label. Possible values = vserver, policylabel
priority	<Integer>	Read-write	Specifies the priority of the policy.
labelname	<String>	Read-write	Name of the responder policy label to which to bind the policy.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/responderpolicylabel_responderpolicy_binding
HTTP Method: PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"responderpolicylabel_responderpolicy_binding":{

<b>"labelname":<String_value>,

</b><b>"policyname":<String_value>,

</b><b>"priority":<Integer_value>,

</b>"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>,

"labeltype":<String_value>,

"invoke_labelname":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/responderpolicylabel_responderpolicy_binding/ labelname_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ responderpolicylabel_responderpolicy_binding/ labelname_value<String> ? **args= policyname:<String_value>, priority: <Integer_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/responderpolicylabel_responderpolicy_binding/ labelname_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ responderpolicylabel_responderpolicy_binding/ labelname_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of responderpolicylabel_responderpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ responderpolicylabel_responderpolicy_binding/ labelname_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the responderpolicylabel_responderpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "responderpolicylabel_responderpolicy_binding": [ {

"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>,

"policyname":<String_value>,

"invoke_labelname":<String_value>,
```

```
"labeltype":<String_value>,

"priority":<Integer_value>,

"labelname":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/responderpolicylabel_responderpolicy_binding
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/responderpolicylabel_responderpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "responderpolicylabel_responderpolicy_binding": [ {

"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>,
```

```
"policyname":<String_value>,

"invoke_labelname":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"labelname":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/responderpolicylabel_responderpolicy_binding/ labelname_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"responderpolicylabel_responderpolicy_binding": [ { "__count": "#no"} ] }
```

rewrite

Rewrite

Rewrite configuration.

NAME	DESCRIPTION
rewriteaction	Configuration for rewrite action
rewriteglobal_binding	Binding object showing the resources that can be bound to rewriteglobal
rewriteglobal_rewritepolicy_binding	Binding object showing the rewritepolicy that can be bound to rewriteglobal
rewriteparam	Configuration for rewrite parameter
rewritepolicy	Configuration for rewrite policy
rewritepolicy_binding	Binding object showing the resources that can be bound to rewritepolicy
rewritepolicy_csvserver_binding	Binding object showing the csvserver that can be bound to rewritepolicy
rewritepolicy_lbvserver_binding	Binding object showing the lbvserver that can be bound to rewritepolicy
rewritepolicy_rewriteglobal_binding	Binding object showing the rewriteglobal that can be bound to rewritepolicy
rewritepolicy_rewritepolicylabel_binding	Binding object showing the rewritepolicylabel that can be bound to rewritepolicy
rewritepolicy_vpnvserver_binding	Binding object showing the vpnvserver that can be bound to rewritepolicy
rewritepolicylabel	Configuration for rewrite policy label

NAME	DESCRIPTION
rewritepolicylabel_binding	Binding object showing the resources that can be bound to rewritepolicylabel
rewritepolicylabel_policybinding_binding	Binding object showing the policybinding that can be bound to rewritepolicylabel
rewritepolicylabel_rewritepolicy_binding	Binding object showing the rewritepolicy that can be bound to rewritepolicylabel

rewriteaction

Configuration for rewrite action resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the user-defined rewrite action. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Can be changed after the rewrite policy is added.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my rewrite action" or 'my rewrite action').
type	<String>	Read-write	Type of user-defined rewrite action. The information that you provide for, and the effect of, each type are as follows:: * REPLACE <target> <string_builder_expr>. Replaces the string with the string-builder expression. * REPLACE_ALL <target> <string_builder_expr> -search <search_expr>. In the request or response specified by <target>, replaces all

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			occurrences of the string defined by <string_builder_expr> with the string defined by <search_expr>. * REPLACE_HTTP_RES <string_builder_expr>. Replaces the complete HTTP response with the string defined by the string-builder expression. * REPLACE_SIP_RES <target> - Replaces the complete SIP response with the string specified by <target>. * INSERT_HTTP_HEADER <header_string_builder_expr> <contents_string_builder_expr>. Inserts the HTTP header specified by <header_string_buil

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			der_expr> and header contents specified by <contents_string_builder_expr>. * DELETE_HTTP_HEADER <target>. Deletes the HTTP header specified by <target>. * CORRUPT_HTTP_HEADER <target>. Replaces the header name of all occurrences of the HTTP header specified by <target> with a corrupted name, so that it will not be recognized by the receiver Example: MY_HEADER is changed to MHEY_ADER. * INSERT_BEFORE <target_expr> <string_builder_expr>. Finds the string specified in <target_expr> and inserts the string in

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			<string_builder_expr> before it. * INSERT_BEFORE_ALL <target> <string_builder_expr> -search <search_expr>. In the request or response specified by <target>, locates all occurrences of the string specified in <string_builder_expr> and inserts the string specified in <search_expr> before each. * INSERT_AFTER <target_expr> <string_builder_expr>. Finds the string specified in <target_expr>, and inserts the string specified in <string_builder_expr> after it. * INSERT_AFTER_ALL <target> <string_builder_expr> -search

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			<search_expr>. In the request or response specified by <target>, locates all occurrences of the string specified by <string_builder_expr> and inserts the string specified by <search_expr> after each. * DELETE <target>. Finds and deletes the specified target. * DELETE_ALL <target> -search <string_builder_expr>. In the request or response specified by <target>, locates and deletes all occurrences of the string specified by <string_builder_expr>. * REPLACE_DIAMETER_HEADER_FIELD <target> <field value>. In the request or response modify the header field specified by

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			<target>. Use Diameter.req.flags. SET(<flag>) or Diameter.req.flags. UNSET<flag> as 'stringbuilderexpression' to set or unset flags. * REPLACE_DNS_HEADER_FIELD <target>. In the request or response modify the header field specified by <target>. * REPLACE_DNS_ANSWER_SECTION <target>. Replace the DNS answer section in the response. This is currently applicable for A and AAAA records only. Use DNS.NEW_RRSET_A ; DNS.NEW_RRSET_AAAA expressions to configure the new answer section.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			* REPLACE_MQTT <target> <string_builder_expr> : Replace MQTT message fields specified in <target_expr> to the value specified in <string_builder_expr> * INSERT_MQTT <string_builder_expr> : Insert the string_builder_expr to an appropriate packet field in the MQTT message. * INSERT_AFTER_MQTT <target_expr> <string_builder_expr> : Insert a topic specified in <string_builder_expr> in the MQTT Subscribe or Unsubscribe message after the specified target_expr. * INSERT_BEFORE_MQTT <target_expr>

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			<string_builder_expr> : Insert a topic specified in <string_builder_expr> in the MQTT Subscribe or Unsubscribe message before the specified target_expr. * DELETE_MQTT <target> : Deletes the specified target in the MQTT message. Possible values = noop, delete, insert_http_header, delete_http_header, corrupt_http_header, insert_before, insert_after, replace, replace_http_res, delete_all, replace_all, insert_before_all, insert_after_all, clientless_vpn_encode, clientless_vpn_encode_all, clientless_vpn_decode, clientless_vpn_deco

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			de_all, insert_sip_header, delete_sip_header, corrupt_sip_header, replace_sip_res, replace_diameter_header_field, replace_dns_header_field, replace_dns_answer_section, replace_mqtt, delete_mqtt, insert_mqtt, insert_before_mqtt, insert_after_mqtt
target	<String>	Read-write	Expression that specifies which part of the request or response to rewrite. Minimum length = 1
stringbuilderexpr	<String>	Read-write	Expression that specifies the content to insert into the request or response at the specified location, or that replaces the specified string.
search	<String>	Read-write	Search facility that is used to match multiple strings in the request or response. Used in the INSERT_BEFORE_ALL,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			INSERT_AFTER_ALL, REPLACE_ALL, and DELETE_ALL action types. The following search types are supported: * Text ("text(string)") - A literal string. Example: -search text("hello") * Regular expression ("regex(re<delimiter>regular exp<delimiter>)") - Pattern that is used to match multiple strings in the request or response. The pattern may be a PCRE-format regular expression with a delimiter that consists of any printable ASCII non-alphanumeric character except for the underscore (_) and space ( ) that is not otherwise used in the expression. Example: -search regex(re~\^hello*~) The preceding regular expression

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			can use the tilde (~) as the delimiter because that character does not appear in the regular expression itself. * XPath ("xpath(xp<delimiter>xpath expression<delimiter>)") - An XPath expression to search XML. The delimiter has the same rules as for regex. Example: -search xpath(xp%/a/b%) * JSON ("xpath_json(xp<delimiter>xpath expression<delimiter>)") - An XPath expression to search JSON. The delimiter has the same rules as for regex. Example: -search xpath_json(xp%/a/b%)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			NOTE: JSON searches use the same syntax as XPath searches, but operate on JSON files instead of standard XML files. * HTML ("xpath_html(xp<delimiter>xpath expression<delimiter>)") - An XPath expression to search HTML. The delimiter has the same rules as for regex. Example: -search xpath_html(xp%/html/body%) NOTE: HTML searches use the same syntax as XPath searches, but operate on HTML files instead of standard XML files; HTML 5 rules for the file syntax are used; HTML 4 and later are supported. * Patset ("patset(patset)") - A predefined pattern

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			set. Example: -search patset("patset1"). * Datset ("dataset(dataset)") - A predefined dataset. Example: -search dataset("dataset1"). * AVP ("avp(avp number)") - AVP number that is used to match multiple AVPs in a Diameter/ Radius Message. Example: -search avp(999) Note: for all these the TARGET prefix can be used in the replacement expression to specify the text that was selected by the -search parameter, optionally adjusted by the -refineSearch parameter. Example: TARGET.BEFORE_STR(",").

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
refinesearch	<String>	Read-write	Specify additional criteria to refine the results of the search. Always starts with the "extend(m,n)" operation, where 'm' specifies number of bytes to the left of selected data and 'n' specifies number of bytes to the right of selected data to extend the selected area. You can use refineSearch only on body expressions, and for the INSERT_BEFORE_ALL, INSERT_AFTER_ALL, REPLACE_ALL, and DELETE_ALL action types. Example: -refineSearch 'EXTEND(10, 20).REGEX_SELECT(re~0x[0-9a-zA-Z]+~).
comment	<String>	Read-write	Comment. Can be used to preserve

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			information about this rewrite action.
newname	<String>	Read-write	New name for the rewrite action. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Can be changed after the rewrite policy is added. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my rewrite action" or 'my rewrite action'). Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
hits	<Integer>	Read-only	The number of times the action has been taken.
undefhits	<Integer>	Read-only	The number of times the action resulted in UNDEF.
referencecount	<Integer>	Read-only	The number of references to the action.
description	<String>	Read-only	Description of the action.
isdefault	<Boolean>	Read-only	A value of true is returned if it is a default rewriteaction.
builtin	<String[]>	Read-only	Flag to determine whether rewrite action is built-in or not. Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL
feature	<String>	Read-only	The feature to be checked while applying this config.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT
- RENAME

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/rewriteaction **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"rewriteaction":{

<b>"name":<String_value>,

</b><b>"type":<String_value>,

</b><b>"target":<String_value>,

</b>"stringbuilderexpr":<String_value>,

"search":<String_value>,

"refinesearch":<String_value>,

"comment":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/rewriteaction/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/rewriteaction **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"rewriteaction":{

<b>"name":<String_value>,

</b>"target":<String_value>,

"stringbuilderexpr":<String_value>,

"search":<String_value>,

"refinesearch":<String_value>,

"comment":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/rewriteaction? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"rewriteaction":{

<b>"name":<String_value>,

</b>"stringbuilderexpr":true,

"refinesearch":true,

"comment":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

RENAME

URL: http:// <netscaler-ip-address> /nitro/v1/config/rewriteaction? **action=rename HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"rewriteaction":{

<b>"name":<String_value>,

</b><b>"newname":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/rewriteaction **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/rewriteaction? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/rewriteaction? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of rewriteaction resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/rewriteaction? **view=summary**

Use this query-parameter to get the summary output of rewriteaction resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/rewriteaction? **pagesize=#no;pageno=#no**

Use this query-parameter to get the rewriteaction resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "rewriteaction": [ {

"name":<String_value>,

"type":<String_value>,

"target":<String_value>,

"stringbuilderexpr":<String_value>,

"search":<String_value>,

"refinesearch":<String_value>,

"hits":<Integer_value>,

"undefhits":<Integer_value>,

"referencecount":<Integer_value>,

"description":<String_value>,

"isdefault":<Boolean_value>,

"comment":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/rewriteaction/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/rewriteaction/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/rewriteaction/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of rewriteaction resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "rewriteaction": [ {

"name":<String_value>,

"type":<String_value>,

"target":<String_value>,

"stringbuilderexpr":<String_value>,

"search":<String_value>,

"refinesearch":<String_value>,

"hits":<Integer_value>,

"undefhits":<Integer_value>,
```

```
"referencecount":<Integer_value>,

"description":<String_value>,

"isdefault":<Boolean_value>,

"comment":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/rewriteaction? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "rewriteaction": [ { "__count": "#no"} ] }
```

rewriteglobal_binding

Binding object which returns the resources bound to rewriteglobal.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
rewriteglobal_rewrite policy_binding	<rewriteglobal_rewrit epolicy_binding[]>	Read-write	rewritepolicy that can be bound to rewriteglobal.

Operations

(click to see Properties)

- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/rewriteglobal_binding

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "rewriteglobal_binding": [ {

"rewriteglobal_rewritepolicy_binding":<rewriteglobal_rewritepolicy_binding
[]_value>

}]}
```

rewriteglobal_rewritepolicy_binding

Binding object showing the rewritepolicy that can be bound to rewriteglobal.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
labelname	<String>	Read-write	* If labelType is policylabel, name of the policy label to invoke. * If labelType is reqvserver or resvserver, name of the virtual server to which to forward the request of response.
priority	<Integer>	Read-write	Specifies the priority of the policy.
labeltype	<String>	Read-write	Type of invocation. Available settings function as follows: * reqvserver - Forward the request to the specified request virtual server. * resvserver - Forward the response to the specified response virtual server. * policylabel - Invoke the specified policy label. Possible values = reqvserver, resvserver, policylabel
policyname	<String>	Read-write	Name of the rewrite policy.
globalbindtype	<String>	Read-write	. Default value: SYSTEM_GLOBAL

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = SYSTEM_GLOBAL, VPN_GLOBAL, RNAT_GLOBAL, APPFW_GLOBAL, TM_GLOBAL
invoke	<Boolean>	Read-write	Terminate evaluation of policies bound to the current policy label, and then forward the request to the specified virtual server or evaluate the specified policy label.
gotopriorityexpression	<String>	Read-write	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
type	<String>	Read-write	The bindpoint to which to policy is bound. Possible values = REQ_OVERRIDE, REQ_DEFAULT, RES_OVERRIDE, RES_DEFAULT, OTHERTCP_REQ_OVERRIDE, OTHERTCP_REQ_DEFAULT, OTHERTCP_RES_OVERRIDE,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			OTHERTCP_RES_DEFAULT, SIPUDP_REQ_OVERRIDE, SIPUDP_REQ_DEFAULT, SIPUDP_RES_OVERRIDE, SIPUDP_RES_DEFAULT, SIPTCP_REQ_OVERRIDE, SIPTCP_REQ_DEFAULT, SIPTCP_RES_OVERRIDE, SIPTCP_RES_DEFAULT, DIAMETER_REQ_OVERRIDE, DIAMETER_REQ_DEFAULT, DIAMETER_RES_OVERRIDE, DIAMETER_RES_DEFAULT, RADIUS_REQ_OVERRIDE, RADIUS_REQ_DEFAULT, RADIUS_RES_OVERRIDE, RADIUS_RES_DEFAULT, DNS_REQ_OVERRIDE,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			DNS_REQ_DEFAULT, DNS_RES_OVERRIDE, DNS_RES_DEFAULT, HTTPQUIC_REQ_OVERRIDE, HTTPQUIC_REQ_DEFAULT, HTTPQUIC_RES_OVERRIDE, HTTPQUIC_RES_DEFAULT, MQTT_REQ_OVERRIDE, MQTT_REQ_DEFAULT, MQTT_RES_OVERRIDE, MQTT_RES_DEFAULT
numpol	<Integer>	Read-only	The number of policies bound to the bindpoint.
flowtype	<Integer>	Read-only	flowtype of the bound rewrite policy.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE

- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/rewriteglobal_rewritepolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"rewriteglobal_rewritepolicy_binding":{

<b>"policyname":<String_value>,

</b><b>"priority":<Integer_value>,

</b>"gotopriorityexpression":<String_value>,

"type":<String_value>,

"invoke":<Boolean_value>,

"labeltype":<String_value>,

"labelname":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/rewriteglobal_rewritepolicy_binding **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/rewriteglobal_rewritepolicy_binding? **args= policyname:<String_value>, type: <String_value> ,priority: <Integer_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/rewriteglobal_rewritepolicy_binding **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/rewriteglobal_rewritepolicy_binding? **args=type: <String_value>**

Use this query-parameter to get rewriteglobal_rewritepolicy_binding resources based on additional properties.

filter http:// <netscaler-ip-address> /nitro/v1/config/rewriteglobal_rewritepolicy_binding? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of rewriteglobal_rewritepolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/rewriteglobal_rewritepolicy_binding? **pagesize=#no;pageno=#no**

Use this query-parameter to get the rewriteglobal_rewritepolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "rewriteglobal_rewritepolicy_binding": [ {

"labelname":<String_value>,

"priority":<Integer_value>,
```

```
"labeltype":<String_value>,

"policyname":<String_value>,

"globalbindtype":<String_value>,

"invoke":<Boolean_value>,

"gotopriorityexpression":<String_value>,

"type":<String_value>,

"numpol":<Integer_value>,

"flowtype":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/rewriteglobal_rewritepolicy_binding?**count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "rewriteglobal_rewritepolicy_binding": [ { "__count": "#no"} ] }
```

rewriteparam

Configuration for rewrite parameter resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
undefaction	<String>	Read-write	Action to perform if the result of policy evaluation is undefined (UNDEF). An UNDEF event indicates an error condition in evaluating the expression. Available settings function as follows: * NOREWRITE - Do not modify the message. * RESET - Reset the connection and notify the user's browser, so that the user can resend the request. * DROP - Drop the message without sending a response to the user. Default value: "NOREWRITE"
timeout	<Integer>	Read-write	Maximum time in milliseconds to allow

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			for processing all the policies and their selected actions without interruption. If the timeout is reached then the evaluation causes an UNDEF to be raised and no further processing is performed. Note that some rewrites may have already been performed. Default value: 3900 Minimum value = 1 Maximum value = 5000
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- UPDATE
- UNSET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/rewriteparam **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"rewriteparam":{

"undefaction":<String_value>,

"timeout":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/rewriteparam? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"rewriteparam":{

"undefaction":true,

"timeout":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/rewriteparam **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "rewriteparam": [ {

"undefaction":<String_value>,

"timeout":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

rewritepolicy

Configuration for rewrite policy resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the rewrite policy. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Can be changed after the rewrite policy is added. The following requirement applies

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my rewrite policy" or 'my rewrite policy').
rule	<String>	Read-write	Expression against which traffic is evaluated. The following requirements apply only to the Citrix ADC CLI: * If the expression includes one or more spaces, enclose the entire expression in double quotation marks. * If the expression itself includes double quotation marks, escape the quotations by using the \ character. * Alternatively, you can use single

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks.
action	<String>	Read-write	Name of the rewrite action to perform if the request or response matches this rewrite policy. There are also some built-in actions which can be used. These are: * NOREWRITE - Send the request from the client to the server or response from the server to the client without making any changes in the message. * RESET - Resets the client connection by closing it. The client program, such as a browser, will handle this and may inform the user. The client may then resend

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			the request if desired. * DROP - Drop the request without sending a response to the user.
undefaction	<String>	Read-write	Action to perform if the result of policy evaluation is undefined (UNDEF). An UNDEF event indicates an internal error condition. Only the above built-in actions can be used.
comment	<String>	Read-write	Any comments to preserve information about this rewrite policy.
logaction	<String>	Read-write	Name of messagelog action to use when a request matches this policy.
newname	<String>	Read-write	New name for the rewrite policy. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space ( ), at (@),

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			equals (=), colon (:), and underscore characters. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my rewrite policy" or 'my rewrite policy'). Minimum length = 1
hits	<Integer>	Read-only	Number of hits.
undefhits	<Integer>	Read-only	Number of Undef hits.
description	<String>	Read-only	Description of the policy.
isdefault	<Boolean>	Read-only	A value of true is returned if it is a default rewritepolicy.
builtin	<String[]>	Read-only	Flag to determine if rewrite policy is built-in or not. Possible values = MODIFIABLE, DELETABLE,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			IMMUTABLE, PARTITION_ALL
feature	<String>	Read-only	The feature to be checked while applying this config.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT
- RENAME

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of

creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/rewritepolicy **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"rewritepolicy":{

<b>"name":<String_value>,

</b><b>"rule":<String_value>,

</b><b>"action":<String_value>,

</b>"undefaction":<String_value>,

"comment":<String_value>,

"logaction":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/rewritepolicy/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/rewritepolicy **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"rewritepolicy":{

<b>"name":<String_value>,

</b>"rule":<String_value>,

"action":<String_value>,

"undefaction":<String_value>,

"comment":<String_value>,

"logaction":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/rewritepolicy? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"rewritepolicy":{

<b>"name":<String_value>,

</b>"undefaction":true,

"comment":true,

"logaction":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

RENAME

URL: http:// <netscaler-ip-address> /nitro/v1/config/rewritepolicy? **action=rename HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"rewritepolicy":{

<b>"name":<String_value>,

</b><b>"newname":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/rewritepolicy **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/rewritepolicy? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/rewritepolicy? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of rewritepolicy resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/rewritepolicy? **view=summary**

Use this query-parameter to get the summary output of rewritepolicy resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/rewritepolicy? **pagesize=#no;pageno=#no**

Use this query-parameter to get the rewritepolicy resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "rewritepolicy": [ {

"name":<String_value>,

"rule":<String_value>,

"action":<String_value>,

"undefaction":<String_value>,

"hits":<Integer_value>,

"undefhits":<Integer_value>,

"description":<String_value>,

"comment":<String_value>,

"logaction":<String_value>,

"isdefault":<Boolean_value>,

"builtin":<String[]_value>,

"feature":<String_value>,
```

```
"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/rewritepolicy/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/rewritepolicy/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/rewritepolicy/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of rewritepolicy resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "rewritepolicy": [ {

"name":<String_value>,
```

```
"rule":<String_value>,

"action":<String_value>,

"undefaction":<String_value>,

"hits":<Integer_value>,

"undefhits":<Integer_value>,

"description":<String_value>,

"comment":<String_value>,

"logaction":<String_value>,

"isdefault":<Boolean_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/rewritepolicy? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "rewritepolicy": [ { "__count": "#no"} ] }
```

rewritepolicy_binding

Binding object which returns the resources bound to rewritepolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the rewrite policy.
rewritepolicy_lbvserver_binding	<rewritepolicy_lbvserver_binding[]>	Read-only	lbvserver that can be bound to rewritepolicy.
rewritepolicy_rewritepolicylabel_binding	<rewritepolicy_rewritepolicylabel_binding[]>	Read-only	rewritepolicylabel that can be bound to rewritepolicy.
rewritepolicy_rewriteglobal_binding	<rewritepolicy_rewriteglobal_binding[]>	Read-only	rewriteglobal that can be bound to rewritepolicy.
rewritepolicy_csvserver_binding	<rewritepolicy_csvserver_binding[]>	Read-only	csvserver that can be bound to rewritepolicy.
rewritepolicy_vpnvserver_binding	<rewritepolicy_vpnvserver_binding[]>	Read-only	vpnvserver that can be bound to rewritepolicy.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/rewritepolicy_binding/ name_value<String>
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "rewritepolicy_binding": [ {

"name":<String_value>,

"rewritepolicy_rewritepolicylabel_binding":<rewritepolicy_rewritepolicylab
el_binding[]_value>,

"rewritepolicy_csvserver_binding":<rewritepolicy_csvserver_binding[]_value
>,

"rewritepolicy_lbvserver_binding":<rewritepolicy_lbvserver_binding[]_value
>,

"rewritepolicy_rewriteglobal_binding":<rewritepolicy_rewriteglobal_binding
[]_value>,

"rewritepolicy_vpnvserver_binding":<rewritepolicy_vpnvserver_binding[]_val
ue>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/rewritepolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/rewritepolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "rewritepolicy_binding": [ {

"name":<String_value>,

"rewritepolicy_rewritepolicylabel_binding":<rewritepolicy_rewritepolicylab
el_binding[]_value>,

"rewritepolicy_csvserver_binding":<rewritepolicy_csvserver_binding[]_value
>,

"rewritepolicy_lbvserver_binding":<rewritepolicy_lbvserver_binding[]_value
>,

"rewritepolicy_rewriteglobal_binding":<rewritepolicy_rewriteglobal_binding
[]_value>,

"rewritepolicy_vpnvserver_binding":<rewritepolicy_vpnvserver_binding[]_val
ue>

}]}
```

rewritepolicy_csvserver_binding

Binding object showing the csvserver that can be bound to rewritepolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the rewrite policy.
boundto	<String>	Read-write	Location where policy is bound.
labelname	<String>	Read-only	Name of the label to invoke if the current policy rule evaluates to TRUE.
gotopriorityexpression	<String>	Read-only	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
activepolicy	<Integer>	Read-only	Indicates whether policy is bound or not.
labeltype	<String>	Read-only	Type of policy label invocation. Possible values = reqvserver, resvserver, policylabel
priority	<Integer>	Read-only	Specifies the priority of the policy.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)

- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/rewritepolicy_csvserver_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ rewritepolicy_csvserver_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of rewritepolicy_csvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/rewritepolicy_csvserver_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the rewritepolicy_csvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "rewritepolicy_csvserver_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"labelname":<String_value>,

"gotopriorityexpression":<String_value>,

"activepolicy":<Integer_value>,

"labeltype":<String_value>,

"priority":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/rewritepolicy_csvserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/rewritepolicy_csvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "rewritepolicy_csvserver_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"labelname":<String_value>,

"gotopriorityexpression":<String_value>,

"activepolicy":<Integer_value>,

"labeltype":<String_value>,

"priority":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/rewritepolicy_csvserver_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"rewritepolicy_csvserver_binding": [ { "__count": "#no"} ] }
```

rewritepolicy_lbvserver_binding

Binding object showing the lbvserver that can be bound to rewritepolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the rewrite policy.
boundto	<String>	Read-write	Location where policy is bound.
labeltype	<String>	Read-only	Type of policy label invocation. Possible values = reqvserver,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			resvserver, policylabel
priority	<Integer>	Read-only	Specifies the priority of the policy.
labelname	<String>	Read-only	Name of the label to invoke if the current policy rule evaluates to TRUE.
gotopriorityexpression	<String>	Read-only	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
activepolicy	<Integer>	Read-only	Indicates whether policy is bound or not.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/rewritepolicy_lbvserver_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ rewritepolicy_lbvserver_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of rewritepolicy_lbvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/rewritepolicy_lbvserver_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the rewritepolicy_lbvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "rewritepolicy_lbvserver_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"labelname":<String_value>,

"gotopriorityexpression":<String_value>,

"activepolicy":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/rewritepolicy_lbvserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/rewritepolicy_lbvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "rewritepolicy_lbvserver_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"labelname":<String_value>,

"gotopriorityexpression":<String_value>,

"activepolicy":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/rewritepolicy_lbvserver_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"rewritepolicy_lbvserver_binding": [ { "__count": "#no"} ] }
```

rewritepolicy_rewriteglobal_binding

Binding object showing the rewriteglobal that can be bound to rewritepolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
boundto	<String>	Read-write	Location where policy is bound.
name	<String>	Read-write	Name of the rewrite policy.
labeltype	<String>	Read-only	Type of policy label invocation. Possible values = reqvserver, resvserver, policylabel
priority	<Integer>	Read-only	Specifies the priority of the policy.
labelname	<String>	Read-only	Name of the label to invoke if the current policy rule evaluates to TRUE.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
gotopriorityexpression	<String>	Read-only	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
activepolicy	<Integer>	Read-only	Indicates whether policy is bound or not.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/rewritepolicy_rewriteglobal_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ rewritepolicy_rewriteglobal_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of rewritepolicy_rewriteglobal_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/rewritepolicy_rewriteglobal_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the rewritepolicy_rewriteglobal_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "rewritepolicy_rewriteglobal_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"labelname":<String_value>,

"gotopriorityexpression":<String_value>,

"activepolicy":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/rewritepolicy_rewriteglobal_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/rewritepolicy_rewriteglobal_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "rewritepolicy_rewriteglobal_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"labelname":<String_value>,

"gotopriorityexpression":<String_value>,

"activepolicy":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/rewritepolicy_rewriteglobal_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"rewritepolicy_rewriteglobal_binding": [ { "__count": "#no"} ] }
```

rewritepolicy_rewritepolicylabel_binding

Binding object showing the rewritepolicylabel that can be bound to rewritepolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the rewrite policy.
boundto	<String>	Read-write	Location where policy is bound.
labelname	<String>	Read-only	Name of the label to invoke if the current policy rule evaluates to TRUE.
gotopriorityexpression	<String>	Read-only	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
activepolicy	<Integer>	Read-only	Indicates whether policy is bound or not.
labeltype	<String>	Read-only	Type of policy label invocation. Possible values = reqvserver, resvserver, policylabel

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
priority	<Integer>	Read-only	Specifies the priority of the policy.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/rewritepolicy_rewritepolicylabel_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ rewritepolicy_rewritepolicylabel_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of rewritepolicy_rewritepolicylabel_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/rewritepolicy_rewritepolicylabel_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the rewritepolicy_rewritepolicylabel_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "rewritepolicy_rewritepolicylabel_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"labelname":<String_value>,

"gotopriorityexpression":<String_value>,

"activepolicy":<Integer_value>,
```

```
"labeltype":<String_value>,

"priority":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/rewritepolicy_rewritepolicylabel_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/rewritepolicy_rewritepolicylabel_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "rewritepolicy_rewritepolicylabel_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"labelname":<String_value>,
```

```
"gotopriorityexpression":<String_value>,

"activepolicy":<Integer_value>,

"labeltype":<String_value>,

"priority":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/rewritepolicy_rewritepolicylabel_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"rewritepolicy_rewritepolicylabel_binding": [ { "__count": "#no"} ] }
```

rewritepolicy_vpnvserver_binding

Binding object showing the vpnvserver that can be bound to rewritepolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the rewrite policy.
boundto	<String>	Read-write	Location where policy is bound.
labelname	<String>	Read-only	Name of the label to invoke if the current policy rule evaluates to TRUE.
gotopriorityexpression	<String>	Read-only	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
activepolicy	<Integer>	Read-only	Indicates whether policy is bound or not.
labeltype	<String>	Read-only	Type of policy label invocation. Possible values = reqvserver, resvserver, policylabel
priority	<Integer>	Read-only	Specifies the priority of the policy.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)

- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/rewritepolicy_vpnvserver_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ rewritepolicy_vpnvserver_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of rewritepolicy_vpnvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/rewritepolicy_vpnvserver_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the rewritepolicy_vpnvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "rewritepolicy_vpnvserver_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"labelname":<String_value>,

"gotopriorityexpression":<String_value>,

"activepolicy":<Integer_value>,

"labeltype":<String_value>,

"priority":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/rewritepolicy_vpnvserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/rewritepolicy_vpnvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "rewritepolicy_vpnvserver_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"labelname":<String_value>,

"gotopriorityexpression":<String_value>,

"activepolicy":<Integer_value>,

"labeltype":<String_value>,

"priority":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/rewritepolicy_vpnvserver_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"rewritepolicy_vpnvserver_binding": [ { "__count": "#no"} ] }
```

rewritepolicylabel

Configuration for rewrite policy label resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
labelname	<String>	Read-write	Name for the rewrite policy label. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space ( ),

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			at (@), equals (=), colon (:), and underscore characters. Cannot be changed after the rewrite policy label is added. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my rewrite policy label" or 'my rewrite policy label').
transform	<String>	Read-write	Types of transformations allowed by the policies bound to the label. For Rewrite, the following types are supported: * http_req - HTTP requests * http_res - HTTP responses * othertcp_req - Non-HTTP TCP requests

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			* othertcp_res - Non-HTTP TCP responses * url - URLs * text - Text strings * clientless_vpn_req - Citrix ADC clientless VPN requests * clientless_vpn_res - Citrix ADC clientless VPN responses * sipudp_req - SIP requests * sipudp_res - SIP responses * diameter_req - DIAMETER requests * diameter_res - DIAMETER responses * radius_req - RADIUS requests * radius_res - RADIUS responses

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			* dns_req - DNS requests * dns_res - DNS responses * mqtt_req - MQTT requests * mqtt_res - MQTT responses. Possible values = http_req, http_res, othertcp_req, othertcp_res, url, text, clientless_vpn_req, clientless_vpn_res, sipudp_req, sipudp_res, siptcp_req, siptcp_res, diameter_req, diameter_res, radius_req, radius_res, dns_req, dns_res, httpquic_req, httpquic_res, mqtt_req, mqtt_res
comment	<String>	Read-write	Any comments to preserve information about this rewrite policy label.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
newname	<String>	Read-write	New name for the rewrite policy label. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space ( ), at (@), equals (=), colon (:), and underscore characters. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my policy label" or 'my policy label'). Minimum length = 1
numpol	<Integer>	Read-only	Number of polices bound to label.
hits	<Integer>	Read-only	Number of times policy label was invoked.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
priority	<Integer>	Read-only	Specifies the priority of the policy.
gotopriorityexpression	<String>	Read-only	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
labeltype	<String>	Read-only	Type of invocation. Available settings function as follows: * reqvserver - Forward the request to the specified request virtual server. * resvserver - Forward the response to the specified response virtual server. * policylabel - Invoke the specified policy label. Possible values = reqvserver, resvserver, policylabel
invoke_labelname	<String>	Read-only	* If labelType is policylabel, name of the policy label to invoke.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			* If labelType is reqvserver or resvserver, name of the virtual server to which to forward the request or response.
flowtype	<Integer>	Read-only	Flowtype of the bound rewrite policy.
description	<String>	Read-only	Description of the policylabel.
isdefault	<Boolean>	Read-only	A value of true is returned if it is a default rewritepolicylabel.
builtin	<String[]>	Read-only	Flag to determine if rewrite policy label is built-in or not. Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL
feature	<String>	Read-only	The feature to be checked while applying this config.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET (ALL)
- GET
- COUNT
- RENAME

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/rewritepolicylabel **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"rewritepolicylabel":{

<b>"labelname":<String_value>,

</b><b>"transform":<String_value>,

</b>"comment":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/rewritepolicylabel/ labelname_value<String>
HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

RENAME

URL: http:// <netscaler-ip-address> /nitro/v1/config/rewritepolicylabel? **action=rename HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"rewritepolicylabel":{

<b>"labelname":<String_value>,

</b><b>"newname":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/rewritepolicylabel **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/rewritepolicylabel? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/rewritepolicylabel? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of rewritepolicylabel resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/rewritepolicylabel? **view=summary**

Use this query-parameter to get the summary output of rewritepolicylabel resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/rewritepolicylabel? **pagesize=#no;pageno=#no**

Use this query-parameter to get the rewritepolicylabel resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "rewritepolicylabel": [ {

"labelname":<String_value>,

"transform":<String_value>,

"numpol":<Integer_value>,

"hits":<Integer_value>,

"priority":<Integer_value>,

"gotopriorityexpression":<String_value>,

"labeltype":<String_value>,

"invoke_labelname":<String_value>,

"flowtype":<Integer_value>,

"description":<String_value>,

"isdefault":<Boolean_value>,

"comment":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,
```

```
"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/rewritepolicylabel/ labelname_value<String>
Query-parameters: attrs http:// <netscaler-ip-address> /nitro/v1/config/rewritepolicylabel/ labelname_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/rewritepolicylabel/ labelname_value<String> ? **view=summary**

Use this query-parameter to get the summary output of rewritepolicylabel resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "rewritepolicylabel": [ {

"labelname":<String_value>,
```

```
"transform":<String_value>,

"numpol":<Integer_value>,

"hits":<Integer_value>,

"priority":<Integer_value>,

"gotopriorityexpression":<String_value>,

"labeltype":<String_value>,

"invoke_labelname":<String_value>,

"flowtype":<Integer_value>,

"description":<String_value>,

"isdefault":<Boolean_value>,

"comment":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/rewritepolicylabel? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "rewritepolicylabel": [ { "__count": "#no"} ] }
```

rewritepolicylabel_binding

Binding object which returns the resources bound to rewritepolicylabel.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
labelname	<String>	Read-write	Name of the rewrite policy label.
rewritepolicylabel_policybinding_binding	<rewritepolicylabel_policybinding_binding[]>	Read-only	policybinding that can be bound to rewritepolicylabel.
rewritepolicylabel_rewritepolicy_binding	<rewritepolicylabel_rewritepolicy_binding[]>	Read-only	rewritepolicy that can be bound to rewritepolicylabel.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/rewritepolicylabel_binding/labelname_value<String>

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "rewritepolicylabel_binding": [ {

"labelname":<String_value>,

"rewritepolicylabel_policybinding_binding":<rewritepolicylabel_policybindi
ng_binding[]_value>,

"rewritepolicylabel_rewritepolicy_binding":<rewritepolicylabel_rewritepoli
cy_binding[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/rewritepolicylabel_binding

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters:

bulkbindings

http:// <netscaler-ip-address> /nitro/v1/config/rewritepolicylabel_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "rewritepolicylabel_binding": [ {

"labelname":<String_value>,

"rewritepolicylabel_policybinding_binding":<rewritepolicylabel_policybindi
ng_binding[]_value>,

"rewritepolicylabel_rewritepolicy_binding":<rewritepolicylabel_rewritepoli
cy_binding[]_value>

}]}
```

rewritepolicylabel_policybinding_binding

Binding object showing the policybinding that can be bound to rewritepolicylabel.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
policyname	<String>	Read-write	Name of the rewrite policy to bind to the policy label.
gotopriorityexpression	<String>	Read-write	Expression specifying the priority of the next policy which will get evaluated if the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			current policy rule evaluates to TRUE.
invoke	<Boolean>	Read-write	Suspend evaluation of policies bound to the current policy label, and then forward the request to the specified virtual server or evaluate the specified policy label.
invoke_labelname	<String>	Read-write	* If labelType is policylabel, name of the policy label to invoke. * If labelType is reqvserver or resvserver, name of the virtual server to which to forward the request or response.
labelname	<String>	Read-write	Name of the rewrite policy label to which to bind the policy.
labeltype	<String>	Read-write	Type of invocation. Available settings function as follows: * reqvserver - Forward the request to the specified request virtual server. * resvserver - Forward the response to the specified response virtual server. * policylabel - Invoke the specified policy label.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = reqvserver, resvserver, policylabel
priority	<Integer>	Read-write	Specifies the priority of the policy.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.
- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/rewritepolicylabel_policybinding_binding/ labelname_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ rewritepolicylabel_policybinding_binding/ labelname_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of rewritepolicylabel_policybinding_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/rewritepolicylabel_policybinding_binding/ labelname_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the rewritepolicylabel_policybinding_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "rewritepolicylabel_policybinding_binding": [ {

"policyname":<String_value>,

"gotopriorityexpression":<String_value>,
```

```
"invoke":<Boolean_value>,

"invoke_labelname":<String_value>,

"labelname":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/rewritepolicylabel_policybinding_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/rewritepolicylabel_policybinding_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "rewritepolicylabel_policybinding_binding": [ {

"policyname":<String_value>,

"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>,

"invoke_labelname":<String_value>,

"labelname":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/rewritepolicylabel_policybinding_binding/ labelname_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"rewritepolicylabel_policybinding_binding": [ { "__count": "#no"} ] }
```

rewritepolicylabel_rewritepolicy_binding

Binding object showing the rewritepolicy that can be bound to rewritepolicylabel.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
invoke_labelname	<String>	Read-write	* If labelType is policylabel, name of the policy label to invoke. * If labelType is reqvserver or resvserver, name of the virtual server to which to forward the request or response.
gotopriorityexpression	<String>	Read-write	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
invoke	<Boolean>	Read-write	Suspend evaluation of policies bound to the current policy label, and then forward the request to the specified virtual server or evaluate the specified policy label.
policyname	<String>	Read-write	Name of the rewrite policy to bind to the policy label.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
labelname	<String>	Read-write	Name of the rewrite policy label to which to bind the policy.
labeltype	<String>	Read-write	Type of invocation. Available settings function as follows: * reqvserver - Forward the request to the specified request virtual server. * resvserver - Forward the response to the specified response virtual server. * policylabel - Invoke the specified policy label. Possible values = reqvserver, resvserver, policylabel
priority	<Integer>	Read-write	Specifies the priority of the policy.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/rewritepolicylabel_rewritepolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"rewritepolicylabel_rewritepolicy_binding":{

<b>"labelname":<String_value>,
```

```
</b><b>"policyname":<String_value>,

</b><b>"priority":<Integer_value>,

</b>"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>,

"labeltype":<String_value>,

"invoke_labelname":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/rewritepolicylabel_rewritepolicy_binding/ labelname_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ rewritepolicylabel_rewritepolicy_binding/ labelname_value<String> ? **args= policyname:<String_value>, priority: <Integer_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/rewritepolicylabel_rewritepolicy_binding/ labelname_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/

rewritepolicylabel_rewritepolicy_binding/ labelname_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of rewritepolicylabel_rewritepolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/rewritepolicylabel_rewritepolicy_binding/ labelname_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the rewritepolicylabel_rewritepolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "rewritepolicylabel_rewritepolicy_binding": [ {

"invoke_labelname":<String_value>,

"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>,

"policyname":<String_value>,

"labelname":<String_value>,

"labeltype":<String_value>,
```

```
"priority":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/rewritepolicylabel_rewritepolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/rewritepolicylabel_rewritepolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "rewritepolicylabel_rewritepolicy_binding": [ {

"invoke_labelname":<String_value>,

"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>,

"policyname":<String_value>,
```

```
"labelname":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/rewritepolicylabel_rewritepolicy_binding/ labelname_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"rewritepolicylabel_rewritepolicy_binding": [ { "__count": "#no"} ] }
```

router

Router

Router configuration.

NAME	DESCRIPTION
accessList	Configuration for accessList resource
bfdInterface	Configuration for bfdInterface resource
bgpPrefix	Configuration for bgpPrefix resource
bgpRouter	Configuration for bgpRouter resource
ipRoute	Configuration for ipRoute resource
ospfDatabase	Configuration for ospfDatabase resource
ospfInterface	Configuration for ospfInterface resource
ospfNeighbor	Configuration for ospfNeighbor resource
ospfRouter	Configuration for ospfRouter resource
ospf6Database	Configuration for ospf6Database resource
ospf6Interface	Configuration for ospf6Interface resource
ospf6Neighbor	Configuration for ospf6Neighbor resource
ospf6Router	Configuration for ospf6Router resource
routeMap	Configuration for routeMap resource
routerdynamicrouting	Configuration for dynamic routing config

accessList

Configuration for accessList resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
id	<String>	Read-write	Standard access list number in the range <0-99> or a ZebOS access-list name.
remark	<String>	Read-write	Access list entry comment.
action	<String>	Read-write	Allow or deny if traffic matches the rule. Possible values: deny, permit
address	<String>	Read-write	Address to match.
wildcard	<String>	Read-write	Wildcard bits.

Operations

(click to see Properties)

- ADD
- SET
- UNSET
- DELETE
- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/routerDynamicRouting/accessList **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"routerDynamicRouting" : {

"accessList" : {

"id" : <String>,

"remark" : <String>,

"rules" : {
```

```
"action" : <String>,

"address" : <String>,

"wildcard" : <String>

}

}

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

SET

URL: http:// <netscaler-ip-address> /nitro/v1/config/routerDynamicRouting/accessList **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"routerDynamicRouting" : {

"accessList" : {

"id" : <String>,

"remark" : <String>,

"rules" : {

"action" : <String>,
```

```
"address" : <String>,

"wildcard" : <String>

}

}

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/routerDynamicRouting/accessList **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"routerDynamicRouting" : {

"accessList" : {

"id" : <String>,

"remark" : true,

"rules" : {

"action" : <String>,

"address" : <String>,
```

```
"wildcard" : <String>

}

}

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/routerDynamicRouting/accessList?args=id:<String> **HTTP Method:** DELETE

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/routerDynamicRouting/accessList **URL:** http:// <netscaler-ip-address> /nitro/v1/config/routerDynamicRouting/accessList?args=id:<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/accessList **?args=id:<String>**

Use this query-parameter to get accessList resources based on additional properties.

HTTP Method: GET

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Payload:

```
{ "routerDynamicRouting": {

"accessList" : [{
```

```
"id" : <String>,

"remark" : <String>,

"rules" : [{

"action" : <String>,

"address" : <String>,

"wildcard" : <String>

}]

}]

}}
```

bfdInterface

Configuration for bfdInterface resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
interval	<Integer>	Read-write	Transmit interval for bfd packets Minimum value: 100 Maximum value: 30000
minrx	<Integer>	Read-write	Minimim receive interval for bfd packets Minimum value: 100

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum value: 30000
multiplier	<Integer>	Read-write	Multiplier for bfd packets Minimum value: 1 Maximum value: 20
name	<String>	Read-write	Name of the interface
passive	<Boolean>	Read-write	Make bfd session passive

Operations

(click to see Properties)

- ADD
- SET
- UNSET
- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.
- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/routerDynamicRouting/bfdInterface **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"routerDynamicRouting" : {

"bfdInterface" : {

"interval" : <Integer>,

"minrx" : <Integer>,

"multiplier" : <Integer>,

<b>"name" : <String></b>,

"passive" : <Boolean>

}

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

SET

URL: http:// <netscaler-ip-address> /nitro/v1/config/routerDynamicRouting/bfdInterface **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"routerDynamicRouting" : {

"bfdInterface" : {

"interval" : <Integer>,

"minrx" : <Integer>,

"multiplier" : <Integer>,

<b>"name" : <String></b>,

"passive" : <Boolean>

}

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/routerDynamicRouting/bfdInterface **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"routerDynamicRouting" : {

"bfdInterface" : {

<b>"name" : <String></b>,

"passive" : true

}

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/routerDynamicRouting/bfdInterface **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/bfdInterface

Use this query-parameter to get bfdInterface resources based on additional properties.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Request Payload:

```
{"routerDynamicRouting" : {
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Payload:

```
{ "routerDynamicRouting": {

"bfdInterface" : [{

"interval" : <Integer>,

"minrx" : <Integer>,

"multiplier" : <Integer>,

"name" : <String>,

"passive" : <Boolean>

}]

}}
```

bgpPrefix

Configuration for bgpPrefix resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ASPath	<String>	Read-write	The set of ASes that must be traversed to reach the network
addressFamily	<String>	Read-write	The address family of the route. Possible values: ipv4, ipv6
attrOrigin	<String>	Read-write	The ultimate origin of the path information. Possible values: IGP, EGP, incomplete
best	<Boolean>	Read-write	Indicates if this is the best route for the prefix.
lastUpdate	<String>	Read-write	Time of last update for the prefix
localPref	<Integer>	Read-write	The originating BGP4 speaker's degree of preference for an advertised route
multiExitDisc	<Integer>	Read-write	This metric is used to discriminate between multiple exit points to an adjacent autonomous system.
nextHop	<String>	Read-write	IP gateway address
peerAddress	<String>	Read-write	The address of the peer router from which the route was learnt.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
prefix	<String>	Read-write	IP destination prefix.
prefixLen	<Integer>	Read-write	IP destination prefix length.

Operations

(click to see Properties)

- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/routerDynamicRouting/bgpPrefix?args=addressFamily:<String> **URL:** http:// <netscaler-ip-address> /nitro/v1/config/routerDynamicRouting/bgpPrefix?args=prefix:<String>,addressFamily:<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/bgpPrefix **?args=prefix:<String>,addressFamily:<String>**

Use this query-parameter to get bgpPrefix resources based on additional properties.

HTTP Method: GET

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Payload:

```
{ "routerDynamicRouting": {

"bgpPrefix" : [{

"ASPath" : <String>,

"addressFamily" : <String>,

"attrOrigin" : <String>,

"best" : <Boolean>,

"lastUpdate" : <String>,

"localPref" : <Integer>,

"multiExitDisc" : <Integer>,

"nextHop" : <String>,

"peerAddress" : <String>,

"prefix" : <String>,

"prefixLen" : <Integer>
```

```
}]

}}
```

bgpRouter

Configuration for bgpRouter resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
addressFamily	<String>	Read-write	Address family of the routes. Possible values: ipv4, ipv6
protocol	<String>	Read-write	The protocol from which routes need to be redistributed. Possible values: kernel, connected, static, rip, ospf, isis, intranet
routeMap	<String>	Read-write	Route map reference
localAS	<Integer>	Read-write	Autonomous system number. Minimum value: 1 Maximum value: 4294967295
ASOriginationInterval	<Integer>	Read-write	Minimum interval between sending AS-origination routing updates.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum value: 1 Maximum value: 65535
address	<String>	Read-write	The ipv4 or ipv6 address of the neighboring router.
advertisementInterval	<Integer>	Read-write	Minimum interval between sending BGP routing updates. Minimum value: 0 Maximum value: 65535
activate	<Boolean>	Read-write	Enable the Address Family for the neighbor.
addressFamily	<String>	Read-write	Address family identifier Possible values: ipv4, ipv6
direction	<String>	Read-write	Apply the route-map to incoming routes or outgoing routes. Possible values: in, out
name	<String>	Read-write	Name of the route-map.
connectTimer	<Integer>	Read-write	Time interval (in seconds) for the ConnectRetry timer. Minimum value: 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum value: 65535
holdTimer	<Integer>	Read-write	Holdtime for the neighbor.
holdTimerConfig	<Integer>	Read-write	Configured hold time for the neighbor. Minimum value: 0 Maximum value: 65535
keepaliveTimer	<Integer>	Read-write	Keepalive time for the neighbor.
keepaliveTimerConfig	<Integer>	Read-write	Configured keepalive time for the neighbor. Minimum value: 0 Maximum value: 65535
localAddress	<String>	Read-write	The local IP address of this entry's BGP connection.
localPort	<Integer>	Read-write	The local port of the TCP connection between the BGP peers.
md5Password	<String>	Read-write	MD5 password for the neighbor.
multihopBfd	<Boolean>	Read-write	Enable BFD for multihop session
remoteAS	<Integer>	Read-write	AS number of the neighbor.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum value: 1 Maximum value: 4294967295
remotePort	<Integer>	Read-write	The remote port of the TCP connection between the BGP peers.
singlehopBfd	<Boolean>	Read-write	Enable BFD on this neighbor
state	<String>	Read-write	The neighbor connection state.
tcpMSS	<Integer>	Read-write	TCP maximum segment size Minimum value: 1 Maximum value: 65535
updateSource	<String>	Read-write	Source of routing updates.
routerId	<String>	Read-write	The router identifier for the bgp routing instance.

Operations

(click to see Properties)

- ADD
- SET
- UNSET
- DELETE
- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/routerDynamicRouting/bgpRouter **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"routerDynamicRouting" : {

"bgpRouter" : {
```

```
"afParams" : {
"addressFamily" : <String>,
"redistribute" : {
"protocol" : <String>,
"routeMap" : <String>
}
},
<b>"localAS" : <Integer></b>,
"neighbor" : {
"ASOriginationInterval" : <Integer>,
"address" : <String>,
"advertisementInterval" : <Integer>,
"afParams" : {
"activate" : <Boolean>,
"addressFamily" : <String>,
"routeMap" : {
"direction" : <String>,
"name" : <String>
}
},
"connectTimer" : <Integer>,
"holdTimerConfig" : <Integer>,
```

```
"keepaliveTimerConfig" : <Integer>,

"md5Password" : <String>,

"multihopBfd" : <Boolean>,

"remoteAS" : <Integer>,

"singlehopBfd" : <Boolean>,

"tcpMSS" : <Integer>,

"updateSource" : <String>

},

"routerId" : <String>

}

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

SET

URL: http:// <netscaler-ip-address> /nitro/v1/config/routerDynamicRouting/bgpRouter **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"routerDynamicRouting" : {

"bgpRouter" : {

"afParams" : {

"addressFamily" : <String>,

"redistribute" : {

"protocol" : <String>,

"routeMap" : <String>

}

},

<b>"localAS" : <Integer></b>,

"neighbor" : {

"ASOriginationInterval" : <Integer>,

"address" : <String>,

"advertisementInterval" : <Integer>,

"afParams" : {

"activate" : <Boolean>,

"addressFamily" : <String>,

"routeMap" : {

"direction" : <String>,

"name" : <String>

}

},
```

```
"connectTimer" : <Integer>,

"holdTimerConfig" : <Integer>,

"keepaliveTimerConfig" : <Integer>,

"md5Password" : <String>,

"multihopBfd" : <Boolean>,

"remoteAS" : <Integer>,

"singlehopBfd" : <Boolean>,

"tcpMSS" : <Integer>,

"updateSource" : <String>

},

"routerId" : <String>

}

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/routerDynamicRouting/bgpRouter **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"routerDynamicRouting" : {

"bgpRouter" : {

"afParams" : {

"addressFamily" : <String>,

"redistribute" : {

"protocol" : <String>,

"routeMap" : true

}

},

<b>"localAS" : <Integer></b>,

"neighbor" : {

"ASOriginationInterval" : true,

"address" : <String>,

"advertisementInterval" : true,

"afParams" : {

"activate" : true,

"addressFamily" : <String>,

"routeMap" : {

"direction" : <String>,

"name" : <String>

}

},
```

```
"connectTimer" : true,

"keepaliveTimerConfig" : true,

"md5Password" : true,

"multihopBfd" : true,

"remoteAS" : <Integer>,

"singlehopBfd" : true,

"tcpMSS" : true,

"updateSource" : true

},

"routerId" : true

}

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/routerDynamicRouting/bgpRouter?args=localAS:<Integer> **HTTP Method:** DELETE

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/routerDynamicRouting/bgpRouter **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/bgpRouter

Use this query-parameter to get bgpRouter resources based on additional properties.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Request Payload:

```
{"routerDynamicRouting" : {
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Payload:

```
{ "routerDynamicRouting": {

"bgpRouter" : [{

"afParams" : [{

"addressFamily" : <String>,

"redistribute" : [{

"protocol" : <String>,

"routeMap" : <String>

}]

}],

"localAS" : <Integer>,
```

```
"neighbor" : [{
"ASOriginationInterval" : <Integer>,
"address" : <String>,
"advertisementInterval" : <Integer>,
"afParams" : [{
"activate" : <Boolean>,
"addressFamily" : <String>,
"routeMap" : [{
"direction" : <String>,
"name" : <String>
}]
}],
"connectTimer" : <Integer>,
"holdTimer" : <Integer>,
"holdTimerConfig" : <Integer>,
"keepaliveTimer" : <Integer>,
"keepaliveTimerConfig" : <Integer>,
"localAddress" : <String>,
"localPort" : <Integer>,
"md5Password" : <String>,
"multihopBfd" : <Boolean>,
"remoteAS" : <Integer>,
```

```
"remotePort" : <Integer>,

"singlehopBfd" : <Boolean>,

"state" : <String>,

"tcpMSS" : <Integer>,

"updateSource" : <String>

}],

"routerId" : <String>

}]

}}
```

ipRoute

Configuration for ipRoute resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
addressFamily	<String>	Read-write	The address family of the route. Possible values: ipv4, ipv6
distance	<Integer>	Read-write	Distance value for this route Minimum value: 1 Maximum value: 255

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
interface	<String>	Read-write	IP gateway interface name or pseudo interface Null
isBest	<Boolean>	Read-write	Indicates is this the best route for the prefix.
metric	<Integer>	Read-write	IP destination prefix.
nextHop	<String>	Read-write	IP gateway address
prefix	<String>	Read-write	IP destination prefix.
prefixLength	<Integer>	Read-write	IP destination prefix length. Minimum value: 0 Maximum value: 128
type	<String>	Read-write	IP route protocol type

Operations

(click to see Properties)

- ADD
- DELETE
- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/routerDynamicRouting/ipRoute **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"routerDynamicRouting" : {

"ipRoute" : {

<b>"addressFamily" : <String></b>,

"distance" : <Integer>,

"interface" : <String>,

"nextHop" : <String>,
```

```
<b>"prefix" : <String></b>,

<b>"prefixLength" : <Integer></b>

}

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/routerDynamicRouting/ipRoute?args=prefixLength:<Integer>,addressFamily:<String>,nextHop:<String>,interface:<String>,prefix:<String>
HTTP Method: DELETE

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/routerDynamicRouting/ipRoute?args=addressFamily:<String> **URL:** http:// <netscaler-ip-address> /nitro/v1/config/routerDynamicRouting/ipRoute?args=prefixLength:<Integer>,addressFamily:<String>,prefix:<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ipRoute **?args=prefixLength:<Integer>,addressFamily:<String>,prefix:<String>**

Use this query-parameter to get ipRoute resources based on additional properties.

HTTP Method: GET

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Payload:

```
{ "routerDynamicRouting": {

"ipRoute" : [{

"addressFamily" : <String>,

"distance" : <Integer>,

"interface" : <String>,

"isBest" : <Boolean>,

"metric" : <Integer>,

"nextHop" : <String>,

"prefix" : <String>,

"prefixLength" : <Integer>,

"type" : <String>

}]

}}
```

ospfDatabase

Configuration for ospfDatabase resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
advRouter	<String>	Read-write	The router ID of the router that originated the LSA into the Autonomous System.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
age	<Integer>	Read-write	The age of the link state advertisement in seconds.
checksum	<Integer>	Read-write	The checksum of the complete contents of the advertisement, excepting the age field
linkId	<String>	Read-write	The link state ID as an IP address.
processId	<Integer>	Read-write	OSPF process ID number
sequenceNo	<Integer>	Read-write	The sequence number of the LSA. The larger the sequence number the more recent the advertisement.
type	<String>	Read-write	The type of LSA

Operations

(click to see Properties)

- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/routerDynamicRouting/ospfDatabase

URL: http:// <netscaler-ip-address> /nitro/v1/config/routerDynamicRouting/ospfDatabase?args=processId:<Integer>

Query-parameters:

args

http:// <netscaler-ip-address> /nitro/v1/config/ospfDatabase **?args=processId:<Integer>**

Use this query-parameter to get ospfDatabase resources based on additional properties.

HTTP Method: GET

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Payload:

```
{ "routerDynamicRouting": {

"ospfDatabase" : [{

"advRouter" : <String>,

"age" : <Integer>,

"checksum" : <Integer>,

"linkId" : <String>,

"processId" : <Integer>,

"sequenceNo" : <Integer>,

"type" : <String>

}]

}}
```

ospfInterface

Configuration for ospfInterface resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
authKey	<String>	Read-write	Authentication password (key).
authType	<String>	Read-write	Authentication type on the ospf interface. Possible values: null, simple, message-digest

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
bfd	<Boolean>	Read-write	Enable bfd on interface
cost	<Integer>	Read-write	Interface cost. Minimum value: 1 Maximum value: 65535
deadInterval	<Integer>	Read-write	Interval after which a neighbor is declared dead Minimum value: 1 Maximum value: 65535
helloInterval	<Integer>	Read-write	Time between HELLO packets Minimum value: 1 Maximum value: 65535
mtu	<Integer>	Read-write	OSPF interface MTU. Minimum value: 576 Maximum value: 65535
name	<String>	Read-write	Name of the interface
networkType	<String>	Read-write	Network type. Possible values: broadcast, non-broadcast, point-to-multipoint, point-to-point

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
priority	<Integer>	Read-write	Router priority. Minimum value: 0 Maximum value: 255
retransmitInterval	<Integer>	Read-write	Time between retransmitting lost link state advertisements. Minimum value: 1 Maximum value: 65535
transmitDelay	<Integer>	Read-write	Link state transmit delay. Minimum value: 1 Maximum value: 65535

Operations

(click to see Properties)

- ADD
- SET
- UNSET
- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/routerDynamicRouting/ospfInterface **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"routerDynamicRouting" : {

"ospfInterface" : {

"authKey" : <String>,

"authType" : <String>,

"bfd" : <Boolean>,

"cost" : <Integer>,
```

```
"deadInterval" : <Integer>,

"helloInterval" : <Integer>,

"mtu" : <Integer>,

<b>"name" : <String></b>,

"networkType" : <String>,

"priority" : <Integer>,

"retransmitInterval" : <Integer>,

"transmitDelay" : <Integer>

}

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

SET

URL: http:// <netscaler-ip-address> /nitro/v1/config/routerDynamicRouting/ospfInterface **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"routerDynamicRouting" : {

"ospfInterface" : {
```

```
"authKey" : <String>,

"authType" : <String>,

"bfd" : <Boolean>,

"cost" : <Integer>,

"deadInterval" : <Integer>,

"helloInterval" : <Integer>,

"mtu" : <Integer>,

<b>"name" : <String></b>,

"networkType" : <String>,

"priority" : <Integer>,

"retransmitInterval" : <Integer>,

"transmitDelay" : <Integer>

}

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/routerDynamicRouting/ospfInterface **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"routerDynamicRouting" : {

"ospfInterface" : {

"authKey" : true,

"authType" : true,

"bfd" : true,

"cost" : true,

"deadInterval" : true,

"helloInterval" : true,

"mtu" : true,

<b>"name" : <String></b>,

"networkType" : true,

"priority" : true,

"retransmitInterval" : true,

"transmitDelay" : true

}

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/routerDynamicRouting/ospfInterface **URL:** http:// <netscaler-ip-address> /nitro/v1/config/routerDynamicRouting/ospfInterface?args=name:<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ospfInterface **?args=name:<String>**

Use this query-parameter to get ospfInterface resources based on additional properties.

HTTP Method: GET

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Payload:

```
{ "routerDynamicRouting": {

"ospfInterface" : [{

"authKey" : <String>,

"authType" : <String>,

"bfd" : <Boolean>,

"cost" : <Integer>,

"deadInterval" : <Integer>,

"helloInterval" : <Integer>,

"mtu" : <Integer>,

"name" : <String>,

"networkType" : <String>,

"priority" : <Integer>,

"retransmitInterval" : <Integer>,
```

```
"transmitDelay" : <Integer>

}]

}}
```

ospfNeighbor

Configuration for ospfNeighbor resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
BDR	<String>	Read-write	The backup designated router for the network.
DR	<String>	Read-write	The designated router for the network.
area	<Integer>	Read-write	The area to which the neighbor belongs.
interface	<String>	Read-write	The interface of peering.
ipaddress	<String>	Read-write	The IP address this neighbor is using in its IP Source Address.
options	<String>	Read-write	The options received from this neighbor.
priority	<Integer>	Read-write	The priority of this neighbor in the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			designated router election algorithm.
processId	<Integer>	Read-write	OSPF process ID number.
routerId	<String>	Read-write	The IpAddress that uniquely identifies the neighboring router in the Autonomous System.
state	<String>	Read-write	The state of the relationship with this neighbor.

Operations

(click to see Properties)

- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/routerDynamicRouting/ospfNeighbor

URL: http:// <netscaler-ip-address> /nitro/v1/config/routerDynamicRouting/ospfNeighbor?args=processId:<Integer>,routerId:<String>

Query-parameters:

args

http:// <netscaler-ip-address> /nitro/v1/config/ospfNeighbor **?**
args=processId:<Integer>,routerId:<String>

Use this query-parameter to get ospfNeighbor resources based on additional properties.

HTTP Method: GET

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Payload:

```
{ "routerDynamicRouting": {

"ospfNeighbor" : [{

"BDR" : <String>,

"DR" : <String>,

"area" : <Integer>,

"interface" : <String>,
```

```
"ipaddress" : <String>,

"options" : <String>,

"priority" : <Integer>,

"processId" : <Integer>,

"routerId" : <String>,

"state" : <String>

}]

}}
```

ospfRouter

Configuration for ospfRouter resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
area	<Integer>	Read-write	OSPF area ID as a decimal value. Minimum value: 0 Maximum value: 4294967295
ipaddress	<String>	Read-write	OSPF network prefix.
netmask	<Integer>	Read-write	The netmask length Minimum value: 0 Maximum value: 32

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
passiveInterface	[<String>]	Read-write	Suppress routing updates on an interface
processId	<Integer>	Read-write	OSPF process ID Minimum value: 1 Maximum value: 65535
metric	<Integer>	Read-write	The metric of redistributed routes. Minimum value: 0 Maximum value: 16777214
metricType	<Integer>	Read-write	OSPF metric type for default routes - OSPF External Type 1 metrics or Type 2 metrics. Minimum value: 1 Maximum value: 2
ospfProcessId	<Integer>	Read-write	The process ID of the ospf instance to redistribute the routes from.
protocol	<String>	Read-write	The protocol from which routes need to be redistributed. Possible values: bgp, connected, intranet, isis, kernel, ospf, rip, static
routeMap	<String>	Read-write	Route map reference

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
tag	<Integer>	Read-write	Set tag for routes redistributed into OSPF Minimum value: 0 Maximum value: 4294967295
routerId	<String>	Read-write	Router-id for the OSPF process

Operations

(click to see Properties)

- ADD
- SET
- UNSET
- DELETE
- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/routerDynamicRouting/ospfRouter **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"routerDynamicRouting" : {

"ospfRouter" : {

"networks" : {

"area" : <Integer>,

"ipaddress" : <String>,

"netmask" : <Integer>

},

"passiveInterface" : [<String>],

<b>"processId" : <Integer></b>,

"redistribute" : {

"metric" : <Integer>,
```

```
"metricType" : <Integer>,

"ospfProcessId" : <Integer>,

"protocol" : <String>,

"routeMap" : <String>,

"tag" : <Integer>

},

"routerId" : <String>

}

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

SET

URL: http:// <netscaler-ip-address> /nitro/v1/config/routerDynamicRouting/ospfRouter **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"routerDynamicRouting" : {

"ospfRouter" : {

"networks" : {
```

```
"area" : <Integer>,

"ipaddress" : <String>,

"netmask" : <Integer>

},

"passiveInterface" : [<String>],

<b>"processId" : <Integer></b>,

"redistribute" : {

"metric" : <Integer>,

"metricType" : <Integer>,

"ospfProcessId" : <Integer>,

"protocol" : <String>,

"routeMap" : <String>,

"tag" : <Integer>

},

"routerId" : <String>

}

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/routerDynamicRouting/ospfRouter **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"routerDynamicRouting" : {

"ospfRouter" : {

"networks" : {

"area" : <Integer>,

"ipaddress" : <String>,

"netmask" : <Integer>

},

"passiveInterface" : [<String>],

<b>"processId" : <Integer></b>,

"redistribute" : {

"metric" : true,

"metricType" : true,

"ospfProcessId" : <Integer>,

"protocol" : <String>,

"routeMap" : true,

"tag" : true
```

```
},

"routerId" : true

}

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/routerDynamicRouting/ospfRouter?args=processId:<Integer> **HTTP Method:** DELETE

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/routerDynamicRouting/ospfRouter **URL:** http:// <netscaler-ip-address> /nitro/v1/config/routerDynamicRouting/ospfRouter?args=processId:<Integer> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ospfRouter **?args=processId:<Integer>**

Use this query-parameter to get ospfRouter resources based on additional properties.

HTTP Method: GET

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Payload:

```
{ "routerDynamicRouting": {

"ospfRouter" : [{

"networks" : [{

"area" : <Integer>,

"ipaddress" : <String>,

"netmask" : <Integer>

}],

"passiveInterface" : [<String>],

"processId" : <Integer>,

"redistribute" : [{

"metric" : <Integer>,

"metricType" : <Integer>,

"ospfProcessId" : <Integer>,

"protocol" : <String>,

"routeMap" : <String>,

"tag" : <Integer>

}],

"routerId" : <String>

}]

}}
```

ospf6Database

Configuration for ospf6Database resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
advRouter	<String>	Read-write	The router ID of the router that originated the LSA into the Autonomous System.
age	<Integer>	Read-write	The age of the link state advertisement in seconds.
checksum	<Integer>	Read-write	The checksum of the complete contents of the advertisement, excepting the age field
linkId	<String>	Read-write	The link state ID as an IP address.
sequenceNo	<Integer>	Read-write	The sequence number of the LSA. The larger the sequence number the more recent the advertisement.
tagId	<String>	Read-write	OSPFv3 process tag
type	<String>	Read-write	The type of LSA

Operations

(click to see Properties)

- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/routerDynamicRouting/ospf6Database

URL: http:// <netscaler-ip-address> /nitro/v1/config/routerDynamicRouting/ospf6Database?args=tagId:<String>

Query-parameters:

args

http:// <netscaler-ip-address> /nitro/v1/config/ospf6Database **?args=tagId:<String>**

Use this query-parameter to get ospf6Database resources based on additional properties.

HTTP Method: GET

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Payload:

```
{ "routerDynamicRouting": {

"ospf6Database" : [{

"advRouter" : <String>,

"age" : <Integer>,

"checksum" : <Integer>,

"linkId" : <String>,

"sequenceNo" : <Integer>,

"tagId" : <String>,

"type" : <String>

}]

}}
```

ospf6Interface

Configuration for ospf6Interface resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
areaId	<Integer>	Read-write	Area on which OSPFv3 is running Minimum value: 0 Maximum value: 4294967295
cost	<Integer>	Read-write	Interface cost. Minimum value: 1 Maximum value: 65535
deadInterval	<Integer>	Read-write	Interval after which a neighbor is declared dead Minimum value: 1 Maximum value: 65535
helloInterval	<Integer>	Read-write	Time between HELLO packets Minimum value: 1 Maximum value: 65535
instanceId	<Integer>	Read-write	Interface Instance Id - <0-31> for v6, <64-95> for v4 Minimum value: 0 Maximum value: 255
name	<String>	Read-write	Name of the interface
networkType	<String>	Read-write	Network type

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values: broadcast, non-broadcast, point-to-multipoint, point-to-point
priority	<Integer>	Read-write	Router priority. Minimum value: 0 Maximum value: 255
retransmitInterval	<Integer>	Read-write	Time between retransmitting lost link state advertisements. Minimum value: 1 Maximum value: 65535
tagId	<String>	Read-write	OSPFv3 Tag
transmitDelay	<Integer>	Read-write	Link state transmit delay. Minimum value: 1 Maximum value: 65535

Operations

(click to see Properties)

- ADD
- SET
- UNSET
- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/routerDynamicRouting/ospf6Interface **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"routerDynamicRouting" : {

"ospf6Interface" : {

"areaId" : <Integer>,
```

```
"cost" : <Integer>,

"deadInterval" : <Integer>,

"helloInterval" : <Integer>,

"instanceId" : <Integer>,

<b>"name" : <String></b>,

"networkType" : <String>,

"priority" : <Integer>,

"retransmitInterval" : <Integer>,

"tagId" : <String>,

"transmitDelay" : <Integer>

}

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

SET

URL: http:// <netscaler-ip-address> /nitro/v1/config/routerDynamicRouting/ospf6Interface **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"routerDynamicRouting" : {

"ospf6Interface" : {

"areaId" : <Integer>,

"cost" : <Integer>,

"deadInterval" : <Integer>,

"helloInterval" : <Integer>,

"instanceId" : <Integer>,

<b>"name" : <String></b>,

"networkType" : <String>,

"priority" : <Integer>,

"retransmitInterval" : <Integer>,

"tagId" : <String>,

"transmitDelay" : <Integer>

}

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/routerDynamicRouting/ospf6Interface **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"routerDynamicRouting" : {

"ospf6Interface" : {

"areaId" : <Integer>,

"cost" : true,

"deadInterval" : true,

"helloInterval" : true,

"instanceId" : <Integer>,

<b>"name" : <String></b>,

"networkType" : <String>,

"priority" : true,

"retransmitInterval" : true,

"tagId" : <String>,

"transmitDelay" : true

}

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/routerDynamicRouting/ospf6Interface **URL:** http:// <netscaler-ip-address> /nitro/v1/config/routerDynamicRouting/ospf6Interface?args=name:<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ospf6Interface **?args=name:<String>**

Use this query-parameter to get ospf6Interface resources based on additional properties.

HTTP Method: GET

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Payload:

```
{ "routerDynamicRouting": {

"ospf6Interface" : [{

"areaId" : <Integer>,

"cost" : <Integer>,

"deadInterval" : <Integer>,

"helloInterval" : <Integer>,

"instanceId" : <Integer>,

"name" : <String>,

"networkType" : <String>,

"priority" : <Integer>,

"retransmitInterval" : <Integer>,

"tagId" : <String>,

"transmitDelay" : <Integer>
```

```
}]

}}
```

ospf6Neighbor

Configuration for ospf6Neighbor resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
BDR	<String>	Read-write	The backup designated router for the network.
DR	<String>	Read-write	The designated router for the network.
area	<Integer>	Read-write	The area to which the neighbor belongs.
interface	<String>	Read-write	The interface of peering.
ip6address	<None>	Read-write	The IP address this neighbor is using in its IP Source Address.
options	<String>	Read-write	The options received from this neighbor.
priority	<Integer>	Read-write	The priority of this neighbor in the designated router election algorithm.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
routerId	<String>	Read-write	The IpAddress that uniquely identifies the neighboring router in the Autonomous System.
state	<String>	Read-write	The state of the relationship with this neighbor.
tagId	<String>	Read-write	OSPFv3 Tag

Operations

(click to see Properties)

- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/routerDynamicRouting/ospf6Neighbor

URL: http:// <netscaler-ip-address> /nitro/v1/config/routerDynamicRouting/ospf6Neighbor?args=tagId:<String>

Query-parameters:

args

http:// <netscaler-ip-address> /nitro/v1/config/ospf6Neighbor **?args=tagId:<String>**

Use this query-parameter to get ospf6Neighbor resources based on additional properties.

HTTP Method: GET

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Payload:

```
{ "routerDynamicRouting": {

"ospf6Neighbor" : [{

"BDR" : <String>,

"DR" : <String>,

"area" : <Integer>,

"interface" : <String>,

"ip6address" : <None>,
```

```
"options" : <String>,

"priority" : <Integer>,

"routerId" : <String>,

"state" : <String>,

"tagId" : <String>

}]

}}
```

ospf6Router

Configuration for ospf6Router resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
addressFamily	<String>	Read-write	IPv4 or IPv6 Address Family Possible values: ipv4, ipv6
metric	<Integer>	Read-write	The metric of redistributed routes. Minimum value: 0 Maximum value: 16777214
metricType	<Integer>	Read-write	OSPFv3 metric type for default routes - OSPFv3 External

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Type 1 metrics or Type 2 metrics. Minimum value: 1 Maximum value: 2
protocol	<String>	Read-write	The protocol from which routes need to be redistributed. Possible values: bgp, connected, isis, kernel, ospf, rip, static
routeMap	<String>	Read-write	Route map reference
tag	<String>	Read-write	Set tag for routes redistributed into OSPFv3
passiveInterface	[<String>]	Read-write	Suppress routing updates on an interface
routerId	<String>	Read-write	Router-id for the OSPFv3 process
tagId	<String>	Read-write	OSPFv3 Tag

Operations

(click to see Properties)

- ADD
- SET
- UNSET
- DELETE
- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/routerDynamicRouting/ospf6Router **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"routerDynamicRouting" : {

"ospf6Router" : {

"afParams" : {
```

```
"addressFamily" : <String>,

"redistribute" : {

"metric" : <Integer>,

"metricType" : <Integer>,

"protocol" : <String>,

"routeMap" : <String>

}

},

"passiveInterface" : [<String>],

"routerId" : <String>,

<b>"tagId" : <String></b>

}

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

SET

URL: http:// <netscaler-ip-address> /nitro/v1/config/routerDynamicRouting/ospf6Router **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"routerDynamicRouting" : {

"ospf6Router" : {

"afParams" : {

"addressFamily" : <String>,

"redistribute" : {

"metric" : <Integer>,

"metricType" : <Integer>,

"protocol" : <String>,

"routeMap" : <String>

}

},

"passiveInterface" : [<String>],

"routerId" : <String>,

<b>"tagId" : <String></b>

}

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/routerDynamicRouting/ospf6Router **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"routerDynamicRouting" : {

"ospf6Router" : {

"afParams" : {

"addressFamily" : <String>,

"redistribute" : {

"metric" : true,

"metricType" : true,

"protocol" : <String>,

"routeMap" : true

}

},

"passiveInterface" : [<String>],

"routerId" : true,

<b>"tagId" : <String></b>

}

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/routerDynamicRouting/ospf6Router?args=tagId:<String> **HTTP Method:** DELETE

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/routerDynamicRouting/ospf6Router **URL:** http:// <netscaler-ip-address> /nitro/v1/config/routerDynamicRouting/ospf6Router?args=tagId:<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ospf6Router **?args=tagId:<String>**

Use this query-parameter to get ospf6Router resources based on additional properties.

HTTP Method: GET

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Payload:

```
{ "routerDynamicRouting": {

"ospf6Router" : [{

"afParams" : [{

"addressFamily" : <String>,

"redistribute" : [{

"metric" : <Integer>,

"metricType" : <Integer>,

"protocol" : <String>,

"routeMap" : <String>,
```

```
"tag" : <String>

}]

}],

"passiveInterface" : [<String>],

"routerId" : <String>,

"tagId" : <String>

}]

}}
```

routeMap

Configuration for routeMap resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Route map tag.
action	<String>	Read-write	Specifies if the route-map denies or permits the operations. Possible values: permit, deny
localPreference	<Integer>	Read-write	Set the BGP local preference path attribute. Minimum value: 0

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum value: 4294967295
matchAsPath	<String>	Read-write	Match the BGP AS-path list.
matchCommunity	<String>	Read-write	Match BGP community list.
matchIpAddress	<String>	Read-write	Match IP address of route. IP access-list number in the range <1-99> or acces-list name.
matchIpNextHop	<String>	Read-write	Match next-hop address of route. IP access-list number in the range <1-99> or acces-list name.
matchMetric	<Integer>	Read-write	Match values from routing table. Match metric of route. Minimum value: 0 Maximum value: 4294967295
matchRouteType	<String>	Read-write	Match OSPF external routes of type 1 or type 2 metrics. Possible values: type-1, type-2
sequence	<Integer>	Read-write	Sequence to insert to/delete from existing route-map entry.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum value: 1 Maximum value: 65535
setAsPath	<String>	Read-write	Set the prepend string for a BGP AS-path attribute
setCommunity	<String>	Read-write	Set the BGP community attribute.
setIpNextHop	<String>	Read-write	Set next hop address of a route.
setMetric	<Integer>	Read-write	Set metric value for destination routing protocol. Minimum value: 0 Maximum value: 4294967295
setMetricType	<String>	Read-write	Set type of metric for destination routing protocol. OSPF external type 1 metric or OSPF external type 2 metric. Possible values: type-1, type-2
weight	<Integer>	Read-write	Set BGP weight for routing table. Minimum value: 0 Maximum value: 4294967295

Operations

(click to see Properties)

- ADD
- SET
- UNSET
- DELETE
- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/routerDynamicRouting/routeMap **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"routerDynamicRouting" : {

"routeMap" : {

<b>"name" : <String></b>,

"rules" : {

<b>"action" : <String></b>,

"localPreference" : <Integer>,

"matchAsPath" : <String>,

"matchCommunity" : <String>,

"matchIpAddress" : <String>,

"matchIpNextHop" : <String>,

"matchMetric" : <Integer>,

"matchRouteType" : <String>,

<b>"sequence" : <Integer></b>,

"setAsPath" : <String>,

"setCommunity" : <String>,

"setIpNextHop" : <String>,

"setMetric" : <Integer>,

"setMetricType" : <String>,

"weight" : <Integer>
```

```
}

}

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

SET

URL: http:// <netscaler-ip-address> /nitro/v1/config/routerDynamicRouting/routeMap **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"routerDynamicRouting" : {

"routeMap" : {

<b>"name" : <String></b>,

"rules" : {

<b>"action" : <String></b>,

"localPreference" : <Integer>,

"matchAsPath" : <String>,

"matchCommunity" : <String>,

"matchIpAddress" : <String>,
```

```
"matchIpNextHop" : <String>,

"matchMetric" : <Integer>,

"matchRouteType" : <String>,

<b>"sequence" : <Integer></b>,

"setAsPath" : <String>,

"setCommunity" : <String>,

"setIpNextHop" : <String>,

"setMetric" : <Integer>,

"setMetricType" : <String>,

"weight" : <Integer>

}

}

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/routerDynamicRouting/routeMap **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"routerDynamicRouting" : {

"routeMap" : {

<b>"name" : <String></b>,

"rules" : {

<b>"action" : <String></b>,

"localPreference" : true,

"matchAsPath" : true,

"matchCommunity" : true,

"matchIpAddress" : true,

"matchIpNextHop" : true,

"matchMetric" : true,

"matchRouteType" : true,

<b>"sequence" : <Integer></b>,

"setAsPath" : true,

"setCommunity" : <String>,

"setIpNextHop" : true,

"setMetric" : true,

"setMetricType" : true,

"weight" : true

}

}

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/routerDynamicRouting/routeMap?args=name:<String> **HTTP Method:** DELETE

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/routerDynamicRouting/routeMap **URL:** http:// <netscaler-ip-address> /nitro/v1/config/routerDynamicRouting/routeMap?args=name:<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/routeMap **?args=name:<String>**

Use this query-parameter to get routeMap resources based on additional properties.

HTTP Method: GET

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Payload:

```
{ "routerDynamicRouting": {

"routeMap" : [{

"name" : <String>,

"rules" : [{

"action" : <String>,
```

```
"localPreference" : <Integer>,

"matchAsPath" : <String>,

"matchCommunity" : <String>,

"matchIpAddress" : <String>,

"matchIpNextHop" : <String>,

"matchMetric" : <Integer>,

"matchRouteType" : <String>,

"sequence" : <Integer>,

"setAsPath" : <String>,

"setCommunity" : <String>,

"setIpNextHop" : <String>,

"setMetric" : <Integer>,

"setMetricType" : <String>,

"weight" : <Integer>

}]

}]

}}
```

routerdynamicrouting

Configuration for dynamic routing config resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
commandstring	<String>	Read-write	command to be executed.
nodeid	<Integer>	Read-write	Unique number that identifies the cluster node. Minimum value = 0 Maximum value = 31
output	<String>	Read-only	command output.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- COUNT
- APPLY

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/routerdynamicrouting **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"routerdynamicrouting":{

"commandstring":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/routerdynamicrouting **Query-parameters: args=commandstring: <String_value>**

update

URL: http:// <netscaler-ip-address> /nitro/v1/config/routerdynamicrouting **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"routerdynamicrouting":{

"commandstring":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

unset

URL: http:// <netscaler-ip-address> /nitro/v1/config/routerdynamicrouting? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"routerdynamicrouting":{

"commandstring":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

apply

URL: http:// <netscaler-ip-address> /nitro/v1/config/routerdynamicrouting? **action=apply HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"routerdynamicrouting":{

"commandstring":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

get (all)

URL: http:// <netscaler-ip-address> /nitro/v1/config/routerdynamicrouting **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/routerdynamicrouting? **args=commandstring: <String_value> ,nodeid: <Integer_value>**

Use this query-parameter to get routerdynamicrouting resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/config/routerdynamicrouting? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/routerdynamicrouting? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of routerdynamicrouting resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/routerdynamicrouting? **view=summary**

Use this query-parameter to get the summary output of routerdynamicrouting resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/routerdynamicrouting? **pagesize=#no;pageno=#no**

Use this query-parameter to get the routerdynamicrouting resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "routerdynamicrouting": [ {

commandstring:<String_value>,nodeid:<Integer_value>"output":<String_value>
,

"_nextgenapiresource":<String_value>

}]}
```

count
URL: http:// <netscaler-ip-address> /nitro/v1/config/routerdynamicrouting? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "routerdynamicrouting": [ { "__count": "#no"} ] }
```

smpp

Smpp

All the commands associated with SMPP.

NAME	DESCRIPTION
smppparam	Configuration for SMPP configuration parameters
smppuser	Configuration for SMPP user

smppparam

Configuration for SMPP configuration parameters resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
clientmode	<String>	Read-write	Mode in which the client binds to the ADC. Applicable settings function as follows: * TRANSCEIVER - Client can send and receive messages to and from the message center. * TRANSMITTERONLY - Client can only send messages. * RECEIVERONLY - Client can only receive messages. Default value: TRANSCEIVER Possible values = TRANSCEIVER, TRANSMITTERONLY, RECEIVERONLY
msgqueue	<String>	Read-write	Queue SMPP messages if a client that is capable of receiving the destination address messages is not available. Default value: OFF

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ON, OFF
msgqueuesize	<Integer>	Read-write	Maximum number of SMPP messages that can be queued. After the limit is reached, the Citrix ADC sends a deliver_sm_resp PDU, with an appropriate error message, to the message center. Default value: 10000
addrton	<Integer>	Read-write	Type of Number, such as an international number or a national number, used in the ESME address sent in the bind request. Default value: 0 Minimum value = 0 Maximum value = 256
addrnpi	<Integer>	Read-write	Numbering Plan Indicator, such as landline, data, or WAP client, used in the ESME address sent in the bind request. Default value: 0

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum value = 0 Maximum value = 256
addrrange	<String>	Read-write	Set of SME addresses, sent in the bind request, serviced by the ESME. Default value: "\\d*"
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- UPDATE
- UNSET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/smppparam **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"smppparam":{

"clientmode":<String_value>,

"msgqueue":<String_value>,

"msgqueuesize":<Integer_value>,

"addrton":<Integer_value>,

"addrnpi":<Integer_value>,

"addrrange":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/smppparam? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"smppparam":{

"clientmode":true,

"msgqueue":true,

"msgqueuesize":true,

"addrton":true,

"addrnpi":true,

"addrrange":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/smppparam **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "smppparam": [ {

"clientmode":<String_value>,

"msgqueue":<String_value>,

"msgqueuesize":<Integer_value>,

"addrton":<Integer_value>,

"addrnpi":<Integer_value>,

"addrrange":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

smppuser

Configuration for SMPP user resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
username	<String>	Read-write	Name of the SMPP user. Must be the same as the user name specified in the SMPP server.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum length = 1
password	<String>	Read-write	Password for binding to the SMPP server. Must be the same as the password specified in the SMPP server. Minimum length = 1
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of

creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/smppuser **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"smppuser":{

<b>"username":<String_value>,

</b>"password":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/smppuser/ username_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/smppuser **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"smppuser":{

<b>"username":<String_value>,

</b>"password":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/smppuser **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/smppuser? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/smppuser? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of smppuser resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/smppuser? **view=summary**

Use this query-parameter to get the summary output of smppuser resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/smppuser? **pagesize=#no;pageno=#no**

Use this query-parameter to get the smppuser resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "smppuser": [ {

"username":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/smppuser/ username_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/smppuser/ username_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/smppuser/ username_value<String> ? **view=summary**

Use this query-parameter to get the summary output of smppuser resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "smppuser": [ {

"username":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/smppuser? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "smppuser": [ { "__count": "#no"} ] }
```

snmp

SNMP

SNMP(Simple Network Management Protocol) configuration.

NAME	DESCRIPTION
snmpalarm	Configuration for alarm
snmpcommunity	Configuration for community
snmpengineid	Configuration for SNMP engine id
snmpgroup	Configuration for SNMP group

NAME	DESCRIPTION
snmpmanager	Configuration for manager
snmpmib	Configuration for SNMP mib
snmpoid	Configuration for SNMP Object Identifier
snmpoption	Configuration for SNMP option
snmptrap	Configuration for snmp trap
snmptrap_binding	Binding object showing the resources that can be bound to snmptrap
snmptrap_snmpuser_binding	Binding object showing the snmpuser that can be bound to snmptrap
snmpuser	Configuration for SNMP user
snmpview	Configuration for view

snmpalarm

Configuration for alarm resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
trapname	<String>	Read-write	Name of the SNMP alarm. This parameter is required for identifying the SNMP

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			alarm and cannot be modified. Possible values = CPU-USAGE, AVERAGE-CPU, MEMORY, MGMT-CPU-USAGE, SYNFLOOD, TCP-SYNFLOOD, VSERVER-REQRATE, SERVICE-REQRATE, ENTITY-RXRATE, ENTITY-TXRATE, ENTITY-SYNFLOOD, SERVICE-MAXCLIENTS, HA-STATE-CHANGE, ENTITY-STATE, CONFIG-CHANGE, CONFIG-SAVE, SERVICEGROUP-MEMBER-REQRATE, SERVICEGROUP-MEMBER-MAXCLIENTS, MONITOR-RTO-THRESHOLD, LOGIN-FAILURE, SSL-CERT-EXPIRY, FAN-SPEED-LOW, VOLTAGE-LOW, VOLTAGE-HIGH,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			TEMPERATURE-HIGH, CPU-TEMPERATURE-HIGH, POWER-SUPPLY-FAILURE, DISK-USAGE-HIGH, INTERFACE-THROUGHPUT-LOW, MON_PROBE_FAILED, HA-VERSION-MISMATCH, HA-DISK-ENCRYPTION-MISMATCH, HA-SYNC-FAILURE, HA-NO-HEARTBEATS, HA-BAD-SECONDARY-STATE, INTERFACE-BW-USAGE, RATE-LIMIT-THRESHOLD-EXCEEDED, ENTITY-NAME-CHANGE, HA-PROP-FAILURE, IP-CONFLICT, PF-RL-RATE-THRESHOLD, PF-RL-PPS-THRESHOLD, PF-RL-RATE-PKTS-DROPPED, PF-RL-PPS-PKTS-

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			DROPPED, APPFW-START-URL, APPFW-DENY-URL, APPFW-VIOLATIONS-TYPE, APPFW-REFERER-HEADER, APPFW-CSRF-TAG, APPFW-COOKIE, APPFW-FIELD-CONSISTENCY, APPFW-BUFFER-OVERFLOW, APPFW-FIELD-FORMAT, APPFW-FILE-UPLOAD-TYPE, APPFW-GRPC, APPFW-GRPC-WEB-JSON, APPFW-GRPC-WEB-TEXT, APPFW-JSON-DOS, APPFW-JSON-SQL, APPFW-JSON-XSS, APPFW-SAFE-COMMERCE, APPFW-SAFE-OBJECT, APPFW-SESSION-LIMIT, APPFW-SIGNATURE-MATCH, APPFW-

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			POLICY-HIT, APPFW-XSS, APPFW-XML-XSS, APPFW-SQL, APPFW-XML-SQL, APPFW-XML-ATTACHMENT, APPFW-XML-DOS, APPFW-XML-VALIDATION, APPFW-XML-WSI, APPFW-XML-SCHEMA-COMPILE, APPFW-XML-SOAP-FAULT, APPFW-NEW-SIGNATURE-ADDED, APPFW-DEPLOY-RELAXATION-DP, APPFW-LEARNED-RULE-APPLIED-DYN-PROF, APPFW-CMD, APPFW-SCHEMA-ENDPOINT-NOTFOUND, APPFW-SCHEMA-METHOD-UNSUPPORTED, APPFW-SCHEMA-PARAMETER-MISSING, APPFW-SCHEMA-VALUE-INCORRECT, APPFW-SCHEMA-

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			CONTENTTYPE-UNSUPPORTED, APPFW-SCHEMA-PARAMETER-INVALID, APPFW-SCHEMA-OTHER, APPFW-SCHEMA-RELAXATION-RULE, APPFW-POSTBODYLIMIT, APPFW-JSON-CMD, APPFW-SQL-GRAM, APPFW-JSON-SQL-GRAM, APPFW-CMD-GRAM, APPFW-JSON-CMD-GRAM, APPFW-BLOCK-KEYWORD, APPFW-JSON-BLOCKKEYWORD, APPFW-BYPASS-LIST, APPFW-DENY-LIST, DNSKEY-EXPIRY, HA-LICENSE-MISMATCH, SSL-CARD-FAILED, SSL-CARD-NORMAL, WARM-RESTART-EVENT, HARD-DISK-DRIVE-ERRORS, COMPACT-FLASH-ERRORS, CALLHOME-

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			UPLOAD-EVENT, 1024KEY-EXCHANGE-RATE, 2048KEY-EXCHANGE-RATE, 4096KEY-EXCHANGE-RATE, SSL-CUR-SESSION-INUSE, CLUSTER-NODE-HEALTH, CLUSTER-NODE-QUORUM, CLUSTER-VERSION-MISMATCH, CLUSTER-CCO-CHANGE, CLUSTER-OVS-CHANGE, CLUSTER-SYNC-FAILURE, CLUSTER-SYNC-PARTIAL-SUCCESS, CLUSTER-PROP-FAILURE, CLUSTER-PROP-EXEC-FAILURE, HA-STICKY-PRIMARY, INBAND-PROTOCOL-VERSION-MISMATCH, SSL-CHIP-REINIT,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			VRID-STATE-CHANGE, PORT-ALLOC-FAILED, LLDP-REMOTE-CHANGE, DUPLICATE-IPV6, PARTITION-CONFIG-EVENT, PARTITION-SWITCHED, LSN-PORTALLOC-FAILED, LSN-PORTQUOTA-EXCEED, LSN-SESSIONQUOTA-EXCEED, LSN-MEM-RECOVERY-KICKEDIN, VSERVER-SPILLOVER, INCONSISTENT-CONFIGURATION-IN-PPES, PARTITION-RATE-LIMIT, POOLED-LICENSE-ONGRACE, POOLED-LICENSE-PARTIAL, CLUSTER-BACKPLANE-HB-MISSING, GSLB-SITE-MEP-FLAP, DNS-MAXNEGCACHE-USAGE, DNS-

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			MAXCACHE-USAGE, NS-LICENSE-EXPIRY, PKT-RATELIMITING-ATTACK, GSLB-SYNC-STATUS-FLIP, URLFILT-DB-UPDATE-STATUS, URLFILT-INIT-SDK, POOLED-LICENSE-CHECKOUT-FAILURE, MIGRATION-STARTED, MIGRATION-COMPLETE, ECDHE-EXCHANGE-RATE, BOT-SIGNATURE-UPDATE, APPFW-XMLPAYLOAD-CONTENT-TYPE-MISMATCH, PORT-ALLOC-EXCEED, KEK_UPDATE_SUCCESS, KEK_UPDATE_FAILURE, ADC-ANOMALY, SYSLOG-CONNECTION-DROPPED, SYSTEM_USER_PASSWORD_EXPIR

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Y_WARNING, DNSSEC-KEY-AUTOMGMT-STATUS-FAILURE, DNSSEC-KEY-AUTOMGMT-STATUS-SUCCESS, CLOUD-REST-API-FAILURE, SSL-ASYM-CRYPTO-UTILIZATION, SSL-SYM-CRYPTO-UTILIZATION, INTERFACE-AUTO-RECOVERY, SYS-KERNEL-ERROR, AVG-MGMT-CPU-USE, EXTRA-MGMT-CPU-USE
thresholdvalue	<Integer>	Read-write	Value for the high threshold. The Citrix ADC generates an SNMP trap message when the value of the attribute associated with the alarm is greater than or equal to the specified high threshold value. Minimum value = 1
normalvalue	<Integer>	Read-write	Value for the normal threshold. A trap message is

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			generated if the value of the respective attribute falls to or below this value after exceeding the high threshold. Minimum value = 1
holdtime	<Integer>	Read-write	Hold time Interval, in seconds, at which the Citrix ADC generates SNMP trap messages when the conditions specified in the SNMP alarm are met recursively for a given period of time. It is recommended to have the hold time interval period in multiple of 7 seconds as the ADC tries to validate the alarms every 7 seconds. Can only be specified for the MGMT-CPU-USAGE alarm. Minimum value = 7
time	<Integer>	Read-write	Interval, in seconds, at which the Citrix ADC generates SNMP trap messages when the conditions specified in the SNMP alarm are met.Can be specified for the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			following alarms: SYNFLOOD, HA-VERSION-MISMATCH, HA-DISK-ENCRYPTION-MISMATCH, HA-SYNC-FAILURE, HA-NO-HEARTBEATS,HA-BAD-SECONDARY-STATE, CLUSTER-NODE-HEALTH, CLUSTER-NODE-QUORUM, CLUSTER-VERSION-MISMATCH, CLUSTER-BKHB-FAILED, PORT-ALLOC-FAILED, COMPACT-FLASH-ERRORS, HARD-DISK-DRIVE-ERRORS and APPFW traps. Default trap time intervals: SYNFLOOD and APPFW traps = 1sec, PORT-ALLOC-FAILED = 3600sec(1 hour), PORT-ALLOC-EXCEED = 3600sec(1 hour), SYSLOG-CONNECTION-DROPPED = 3600sec(1 hour), Other Traps = 86400sec(1 day).

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: 1
state	<String>	Read-write	Current state of the SNMP alarm. The Citrix ADC generates trap messages only for SNMP alarms that are enabled. Some alarms are enabled by default, but you can disable them. Default value: ENABLED Possible values = ENABLED, DISABLED
severity	<String>	Read-write	Severity level assigned to trap messages generated by this alarm. The severity levels are, in increasing order of severity, Informational, Warning, Minor, Major, and Critical. This parameter is useful when you want the Citrix ADC to send trap messages to a trap listener on the basis of severity level. Trap messages with a severity level lower than the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			specified level (in the trap listener entry) are not sent. Default value: Unknown Possible values = Critical, Major, Minor, Warning, Informational
logging	<String>	Read-write	Logging status of the alarm. When logging is enabled, the Citrix ADC logs every trap message that is generated for this alarm. Default value: ENABLED Possible values = ENABLED, DISABLED
timeout	<Integer>	Read-only	If DB is enabled and clear config is fired, then to reset timeinterval of alarm, corresponding default time value is needed. This hidden argument holds the default time value for the corresponding alarm.
_nextgenapiresource	<String>	Read-only	.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- UPDATE
- UNSET
- ENABLE
- DISABLE
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/snmpalarm **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"snmpalarm":{

<b>"trapname":<String_value>,

</b>"thresholdvalue":<Integer_value>,

"normalvalue":<Integer_value>,

"holdtime":<Integer_value>,

"time":<Integer_value>,

"state":<String_value>,

"severity":<String_value>,

"logging":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/snmpalarm? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"snmpalarm":{

<b>"trapname":<String_value>,

</b>"thresholdvalue":true,

"normalvalue":true,

"time":true,

"holdtime":true,

"state":true,

"severity":true,

"logging":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

ENABLE

URL: http:// <netscaler-ip-address> /nitro/v1/config/snmpalarm? **action=enable HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"snmpalarm":{

<b>"trapname":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DISABLE

URL: http:// <netscaler-ip-address> /nitro/v1/config/snmpalarm? **action=disable HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"snmpalarm":{

<b>"trapname":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/snmpalarm **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/snmpalarm? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/snmpalarm? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of snmpalarm resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/snmpalarm? **view=summary**

Use this query-parameter to get the summary output of snmpalarm resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/snmpalarm? **pagesize=#no;pageno=#no**

Use this query-parameter to get the snmpalarm resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "snmpalarm": [ {

"trapname":<String_value>,

"thresholdvalue":<Integer_value>,
```

```
"normalvalue":<Integer_value>,

"time":<Integer_value>,

"holdtime":<Integer_value>,

"state":<String_value>,

"severity":<String_value>,

"logging":<String_value>,

"timeout":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/snmpalarm/ trapname_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/snmpalarm/ trapname_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/snmpalarm/ trapname_value<String> ? **view=summary**

Use this query-parameter to get the summary output of snmpalarm resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "snmpalarm": [ {

"trapname":<String_value>,

"thresholdvalue":<Integer_value>,

"normalvalue":<Integer_value>,

"time":<Integer_value>,

"holdtime":<Integer_value>,

"state":<String_value>,

"severity":<String_value>,

"logging":<String_value>,

"timeout":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/snmpalarm? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "snmpalarm": [ { "__count": "#no"} ] }
```

snmpcommunity

Configuration for community resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
communityname	<String>	Read-write	The SNMP community string. Can consist of 1 to 32 characters that include uppercase and lowercase letters,numbers and special characters. The following requirement applies only to the Citrix ADC CLI: If the string includes one or more spaces, enclose the name in double or single quotation marks (for example,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			"my string" or 'my string'). Minimum length = 1
permissions	<String>	Read-write	The SNMP V1 or V2 query-type privilege that you want to associate with this SNMP community. Possible values = GET, GET_NEXT, GET_BULK, SET, ALL
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/snmpcommunity **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"snmpcommunity":{

<b>"communityname":<String_value>,

</b><b>"permissions":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/snmpcommunity/ communityname_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/snmpcommunity **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/snmpcommunity? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/snmpcommunity? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of snmpcommunity resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/snmpcommunity? **view=summary**

Use this query-parameter to get the summary output of snmpcommunity resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/snmpcommunity? **pagesize=#no;pageno=#no**

Use this query-parameter to get the snmpcommunity resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "snmpcommunity": [ {

"communityname":<String_value>,

"permissions":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/snmpcommunity/ communityname_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/ config/snmpcommunity/ communityname_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/snmpcommunity/ communityname_value<String> ? **view=summary**

Use this query-parameter to get the summary output of snmpcommunity resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "snmpcommunity": [ {

"communityname":<String_value>,

"permissions":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/snmpcommunity? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "snmpcommunity": [ { "__count": "#no"} ] }
```

snmpengineid

Configuration for SNMP engine id resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
engineid	<String>	Read-write	A hexadecimal value of at least 10 characters, uniquely identifying the engineid. Minimum length = 10 Maximum length = 31
ownernode	<Integer>	Read-write	ID of the cluster node for which you are setting the engineid. Default value: -1 Minimum value = 0 Maximum value = 31
defaultengineid	<String>	Read-only	Unique identifier to assign to the SNMPv3 engine. Should be a hexadecimal value with a minimum length of 10 hex characters.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/snmpengineid **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"snmpengineid":{

<b>"engineid":<String_value>,

</b>"ownernode":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/snmpengineid? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"snmpengineid":{

"ownernode":<Integer_value>
```

```
}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/snmpengineid **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/snmpengineid? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/snmpengineid? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of snmpengineid resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/snmpengineid? **view=summary**

Use this query-parameter to get the summary output of snmpengineid resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/snmpengineid? **pagesize=#no;pageno=#no**

Use this query-parameter to get the snmpengineid resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "snmpengineid": [ {

"ownernode":<Integer_value>,

"engineid":<String_value>,

"defaultengineid":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/snmpengineid/ ownernode_value<Integer>
Query-parameters: attrs http:// <netscaler-ip-address> /nitro/v1/config/snmpengineid/ ownernode_value<Integer> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/snmpengineid/ ownernode_value<Integer> ? **view=summary**

Use this query-parameter to get the summary output of snmpengineid resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "snmpengineid": [ {

"ownernode":<Integer_value>,

"engineid":<String_value>,

"defaultengineid":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/snmpengineid? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "snmpengineid": [ { "__count": "#no"} ] }
```

snmpgroup

Configuration for SNMP group resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the SNMPv3 group. Can consist of 1 to 31 characters that include uppercase and lowercase letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore (_) characters. You should choose a name that helps identify the SNMPv3 group. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose it in double or single quotation marks (for example, "my

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			name" or 'my name'). Minimum length = 1
securitylevel	<String>	Read-write	Security level required for communication between the Citrix ADC and the SNMPv3 users who belong to the group. Specify one of the following options: noAuthNoPriv. Require neither authentication nor encryption. authNoPriv. Require authentication but no encryption. authPriv. Require authentication and encryption. Note: If you specify authentication, you must specify an encryption algorithm when you assign an SNMPv3 user to the group. If you also specify encryption, you must assign both an authentication and an encryption

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			algorithm for each group member. Possible values = noAuthNoPriv, authNoPriv, authPriv
readviewname	<String>	Read-write	Name of the configured SNMPv3 view that you want to bind to this SNMPv3 group. An SNMPv3 user bound to this group can access the subtrees that are bound to this SNMPv3 view as type INCLUDED, but cannot access the ones that are type EXCLUDED. If the Citrix ADC has multiple SNMPv3 view entries with the same name, all such entries are associated with the SNMPv3 group. Minimum length = 1
storagetype	<String>	Read-only	The storage type for this group. Possible values = volatile, nonVolatile
status	<String>	Read-only	The status of this group. Possible values = active

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/snmpgroup **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"snmpgroup":{

<b>"name":<String_value>,

</b><b>"securitylevel":<String_value>,

</b><b>"readviewname":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/snmpgroup/ name_value<String> **Query-parameters: args= securitylevel:<String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/snmpgroup **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"snmpgroup":{

<b>"name":<String_value>,

</b><b>"securitylevel":<String_value>,

</b><b>"readviewname":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/snmpgroup **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/snmpgroup? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/snmpgroup? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of snmpgroup resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/snmpgroup? **view=summary**

Use this query-parameter to get the summary output of snmpgroup resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/snmpgroup? **pagesize=#no;pageno=#no**

Use this query-parameter to get the snmpgroup resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "snmpgroup": [ {

"name":<String_value>,

"securitylevel":<String_value>,

"readviewname":<String_value>,

"storagetype":<String_value>,

"status":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/snmpgroup? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "snmpgroup": [ { "__count": "#no"} ] }
```

snmpmanager

Configuration for manager resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ipaddress	<String>	Read-write	IP address of the SNMP manager. Can be an IPv4 or IPv6 address. You can instead specify an IPv4 network address or IPv6 network prefix if you want the Citrix ADC to respond to SNMP queries from any

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			device on the specified network. Alternatively, instead of an IPv4 address, you can specify a host name that has been assigned to an SNMP manager. If you do so, you must add a DNS name server that resolves the host name of the SNMP manager to its IP address. Note: The Citrix ADC does not support host names for SNMP managers that have IPv6 addresses. Minimum length = 1 Maximum length = 255
netmask	<String>	Read-write	Subnet mask associated with an IPv4 network address. If the IP address specifies the address or host name of a specific host, accept the default value of 255.255.255.255.
domainresolveretry	<Integer>	Read-write	Amount of time, in seconds, for which the Citrix ADC waits before sending

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			another DNS query to resolve the host name of the SNMP manager if the last query failed. This parameter is valid for host-name based SNMP managers only. After a query succeeds, the TTL determines the wait time. The minimum and default value is 5. Minimum value = 5 Maximum value = 20939
ip	<String>	Read-only	The resolved IP address of the hostname manager.
domain	<String>	Read-only	IP address of manager. It will be zero for hostname manager.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET

- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/snmpmanager **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"snmpmanager":{

<b>"ipaddress":<String_value>,

</b>"netmask":<String_value>,

"domainresolveretry":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/snmpmanager/ ipaddress_value<String>
Query-parameters: args=netmask: <String_value>
update
URL: http:// <netscaler-ip-address> /nitro/v1/config/snmpmanager **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"snmpmanager":{

<b>"ipaddress":<String_value>,

</b>"netmask":<String_value>,

"domainresolveretry":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error
unset
URL: http:// <netscaler-ip-address> /nitro/v1/config/snmpmanager? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"snmpmanager":{

<b>"ipaddress":<String_value>,

</b>"netmask":<String_value>,

"domainresolveretry":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error
get (all)
URL: http:// <netscaler-ip-address> /nitro/v1/config/snmpmanager **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/snmpmanager? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/snmpmanager? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of snmpmanager resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/snmpmanager? **view=summary**

Use this query-parameter to get the summary output of snmpmanager resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/snmpmanager?**pagesize=#no;pageno=#no**

Use this query-parameter to get the snmpmanager resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "snmpmanager": [ {

"ipaddress":<String_value>,

"netmask":<String_value>,

"ip":<String_value>,

"domain":<String_value>,

"domainresolveretry":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

count

URL: http:// <netscaler-ip-address> /nitro/v1/config/snmpmanager? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "snmpmanager": [ { "__count": "#no"} ] }
```

snmpmib

Configuration for SNMP mib resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
contact	<String>	Read-write	Name of the administrator for this Citrix ADC. Along with the name, you can include information on how to contact this person, such as a

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			phone number or an email address. Can consist of 1 to 127 characters that include uppercase and lowercase letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore (_) characters. The following requirement applies only to the Citrix ADC CLI: If the information includes one or more spaces, enclose it in double or single quotation marks (for example, "my contact" or 'my contact'). Default value: "WebMaster (default)" Minimum length = 1
name	<String>	Read-write	Name for this Citrix ADC. Can consist of 1 to 127 characters that include uppercase and lowercase letters,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore (_) characters. You should choose a name that helps identify the Citrix ADC appliance. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose it in double or single quotation marks (for example, "my name" or 'my name'). Default value: "NetScaler" Minimum length = 1
location	<String>	Read-write	Physical location of the Citrix ADC. For example, you can specify building name, lab number, and rack number. Can consist of 1 to 127 characters that include uppercase and lowercase

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore (_) characters. The following requirement applies only to the Citrix ADC CLI: If the location includes one or more spaces, enclose it in double or single quotation marks (for example, "my location" or 'my location'). Default value: "POP (default)" Minimum length = 1
customid	<String>	Read-write	Custom identification number for the Citrix ADC. Can consist of 1 to 127 characters that include uppercase and lowercase letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore (_)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			characters. You should choose a custom identification that helps identify the Citrix ADC appliance. The following requirement applies only to the Citrix ADC CLI: If the ID includes one or more spaces, enclose it in double or single quotation marks (for example, "my ID" or 'my ID'). Default value: "Default" Minimum length = 1
ownernode	<Integer>	Read-write	ID of the cluster node for which we are setting the mib. This is a mandatory argument to set snmp mib on CLIP. Default value: -1 Minimum value = 0 Maximum value = 31
sysdesc	<String>	Read-only	The description of the system.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
sysuptime	<Integer>	Read-only	The UP time of the system in 100th of a second.
sysservices	<Integer>	Read-only	The services offered by the system.
sysoid	<String>	Read-only	The OID of the system's management system.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of

creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/snmpmib **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"snmpmib":{

"contact":<String_value>,

"name":<String_value>,

"location":<String_value>,

"customid":<String_value>,

"ownernode":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/snmpmib? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"snmpmib":{

"contact":true,

"name":true,

"location":true,

"customid":true,

"ownernode":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/snmpmib **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/snmpmib? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/snmpmib? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of snmpmib resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/snmpmib? **view=summary**

Use this query-parameter to get the summary output of snmpmib resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/snmpmib? **pagesize=#no;pageno=#no**

Use this query-parameter to get the snmpmib resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "snmpmib": [ {

"ownernode":<Integer_value>,

"contact":<String_value>,

"name":<String_value>,

"location":<String_value>,

"sysdesc":<String_value>,
```

```
"sysuptime":<Integer_value>,

"sysservices":<Integer_value>,

"sysoid":<String_value>,

"customid":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/snmpmib/ ownernode_value<Integer> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/snmpmib/ ownernode_value<Integer> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/snmpmib/ ownernode_value<Integer> ? **view=summary**

Use this query-parameter to get the summary output of snmpmib resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "snmpmib": [ {

"ownernode":<Integer_value>,

"contact":<String_value>,

"name":<String_value>,

"location":<String_value>,

"sysdesc":<String_value>,

"sysuptime":<Integer_value>,

"sysservices":<Integer_value>,

"sysoid":<String_value>,

"customid":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/snmpmib? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "snmpmib": [ { "__count": "#no"} ] }
```

snmpoid

Configuration for SNMP Object Identifier resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
entitytype	<String>	Read-write	The type of entity whose SNMP OIDs you want to displayType of entity whose SNMP OIDs you want the Citrix ADC to display. Possible values = VSERVER, SERVICE, SERVICEGROUP
name	<String>	Read-write	Name of the entity whose SNMP OID you want the Citrix ADC to display. Minimum length = 1
Snmpoid	<String>	Read-only	The snmp oid.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/snmpoid **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/snmpoid? **args= entitytype:<String_value>, name: <String_value>**

Use this query-parameter to get snmpoid resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/config/snmpoid? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/snmpoid? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of snmpoid resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/snmpoid? **view=summary**

Use this query-parameter to get the summary output of snmpoid resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/snmpoid? **pagesize=#no;pageno=#no**

Use this query-parameter to get the snmpoid resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "snmpoid": [ {

<b>entitytype:<String_value>,</
b>name:<String_value>"Snmpoid":<String_value>,

"_nextgenapiresource":<String_value>
```

```
}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/snmpoid? **args= entitytype:<String_value>, name: <String_value> ;count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "snmpoid": [ { "__count": "#no"} ] }
```

snmpoption

Configuration for SNMP option resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
snmpset	<String>	Read-write	Accept SNMP SET requests sent to the Citrix ADC, and allow SNMP managers to write values to MIB objects that are

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			configured for write access. Default value: DISABLED Possible values = ENABLED, DISABLED
snmptraplogging	<String>	Read-write	Log any SNMP trap events (for SNMP alarms in which logging is enabled) even if no trap listeners are configured. With the default setting, SNMP trap events are logged if at least one trap listener is configured on the appliance. Default value: DISABLED Possible values = ENABLED, DISABLED
partitionnameintrap	<String>	Read-write	Send partition name as a varbind in traps. By default the partition names are not sent as a varbind. Default value: DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ENABLED, DISABLED
snmptraploggingl evel	<String>	Read-write	Audit log level of SNMP trap logs. The default value is INFORMATIONAL. Default value: INFORMATIONAL Possible values = EMERGENCY, ALERT, CRITICAL, ERROR, WARNING, NOTICE, INFORMATIONAL, DEBUG
severityinfointrap	<String>	Read-write	By default, the severity level info of the trap is not mentioned in the trap message. Enable this option to send severity level of trap as one of the varbind in the trap message. Default value: DISABLED Possible values = ENABLED, DISABLED
customtrap	<String>	Read-write	By default, Customtrap will be disabled, set to

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			enabled when using the feature. Default value: DISABLED Possible values = ENABLED, DISABLED
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- UPDATE
- UNSET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/snmpoption **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"snmpoption":{

"snmpset":<String_value>,

"snmptraplogging":<String_value>,

"partitionnameintrap":<String_value>,

"snmptraploggginglevel":<String_value>,

"severityinfointrap":<String_value>,

"customtrap":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/snmpoption? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"snmpoption":{

"snmpset":true,

"snmptraplogging":true,

"partitionnameintrap":true,

"snmptraploggginglevel":true,

"severityinfointrap":true,

"customtrap":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/snmpoption **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "snmpoption": [ {

"snmpset":<String_value>,

"snmptraplogging":<String_value>,

"partitionnameintrap":<String_value>,

"snmptraploggginglevel":<String_value>,

"severityinfointrap":<String_value>,

"customtrap":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

snmptrap

Configuration for snmp trap resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
trapclass	<String>	Read-write	Type of trap messages that the Citrix ADC sends to the trap listener: Generic or the enterprise-specific messages defined in the MIB file. Possible values = generic, specific

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
trapdestination	<String>	Read-write	IPv4 or the IPv6 address of the trap listener to which the Citrix ADC is to send SNMP trap messages. Minimum length = 1
version	<String>	Read-write	SNMP version, which determines the format of trap messages sent to the trap listener. This setting must match the setting on the trap listener. Otherwise, the listener drops the trap messages. Default value: V2 Possible values = V1, V2, V3
td	<Integer>	Read-write	Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0. Minimum value = 0

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum value = 4094
destport	<Integer>	Read-write	UDP port at which the trap listener listens for trap messages. This setting must match the setting on the trap listener. Otherwise, the listener drops the trap messages. Default value: 162 Minimum value = 1 Maximum value = 65534
communityname	<String>	Read-write	Password (string) sent with the trap messages, so that the trap listener can authenticate them. Can include 1 to 32 uppercase or lowercase letters, numbers, and hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore (_) characters. You must specify the same community string on the trap listener device. Otherwise,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			the trap listener drops the trap messages. The following requirement applies only to the Citrix ADC CLI: If the string includes one or more spaces, enclose the name in double or single quotation marks (for example, "my string" or 'my string').
srcip	<String>	Read-write	IPv4 or IPv6 address that the Citrix ADC inserts as the source IP address in all SNMP trap messages that it sends to this trap listener. By default this is the appliance's NSIP or NSIP6 address, but you can specify an IPv4 MIP or SNIP/ SNIP6 address. In cluster setup, the default value is the individual node's NSIP, but it can be set to CLIP or Striped SNIP address. In non default partition, this

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			parameter must be set to the SNIP/ SNIP6 address. Minimum length = 1
severity	<String>	Read-write	Severity level at or above which the Citrix ADC sends trap messages to this trap listener. The severity levels, in increasing order of severity, are Informational, Warning, Minor, Major, Critical. This parameter can be set for trap listeners of type SPECIFIC only. The default is to send all levels of trap messages. Important: Trap messages are not assigned severity levels unless you specify severity levels when configuring SNMP alarms. Default value: Unknown Possible values = Critical, Major, Minor, Warning, Informational

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
allpartitions	<String>	Read-write	Send traps of all partitions to this destination. Default value: DISABLED Possible values = ENABLED, DISABLED
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.
- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of

creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/snmptrap **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"snmptrap":{

<b>"trapclass":<String_value>,

</b><b>"trapdestination":<String_value>,

</b>"version":<String_value>,

"td":<Integer_value>,

"destport":<Integer_value>,

"communityname":<String_value>,

"srcip":<String_value>,

"severity":<String_value>,
```

```
"allpartitions":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/snmptrap/ trapclass_value<String> **Query-parameters: args= trapdestination:<String_value>, version: <String_value> ,td: <Integer_value>**
update
URL: http:// <netscaler-ip-address> /nitro/v1/config/snmptrap **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"snmptrap":{

<b>"trapclass":<String_value>,

</b><b>"trapdestination":<String_value>,

</b>"version":<String_value>,

"td":<Integer_value>,

"destport":<Integer_value>,

"communityname":<String_value>,

"srcip":<String_value>,

"severity":<String_value>,
```

```
"allpartitions":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

unset

URL: http:// <netscaler-ip-address> /nitro/v1/config/snmptrap? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"snmptrap":{

<b>"trapclass":<String_value>,

</b><b>"trapdestination":<String_value>,

</b>"version":<String_value>,

"td":<Integer_value>,

"destport":true,

"communityname":true,

"srcip":true,

"severity":true,

"allpartitions":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error
get (all)
URL: http:// <netscaler-ip-address> /nitro/v1/config/snmptrap **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/snmptrap? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/snmptrap? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of snmptrap resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/snmptrap? **view=summary**

Use this query-parameter to get the summary output of snmptrap resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/snmptrap? **pagesize=#no;pageno=#no**

Use this query-parameter to get the snmptrap resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "snmptrap": [ {

"trapclass":<String_value>,

"trapdestination":<String_value>,

"version":<String_value>,

"td":<Integer_value>,

"destport":<Integer_value>,

"communityname":<String_value>,

"srcip":<String_value>,

"severity":<String_value>,

"allpartitions":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

count

URL: http:// <netscaler-ip-address> /nitro/v1/config/snmptrap? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "snmptrap": [ { "__count": "#no"} ] }
```

snmptrap_binding

Binding object which returns the resources bound to snmptrap.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
trapclass	<String>	Read-write	Trap type specified in the trap listener entry. Possible values = generic, specific
trapdestination	<String>	Read-write	IP address specified in the trap listener entry. Minimum length = 1
version	<String>	Read-write	The SNMP version of the trap specified in the trap listener entry. Possible values = V1, V2, V3
td	<Integer>	Read-write	Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			domain, which has an ID of 0. Minimum value = 0 Maximum value = 4094
snmptrap_snmpuser_binding	<snmptrap_snmpuser_binding[]>	Read-only	snmpuser that can be bound to snmptrap.

Operations

(click to see Properties)

- GET (BY ARGS)
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/snmptrap_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: args http:// <netscaler-ip-address> /nitro/v1/config/snmptrap_binding?
args=trapclass:<String_value>,trapdestination:<String_value>,version:<String_value>,td:<Integer_valu

Use this query-parameter to get snmptrap_binding resources based on additional properties.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "snmptrap_binding": [ {

"trapclass":<String_value>,

"trapdestination":<String_value>,

"version":<String_value>,

"td":<Integer_value>,

"snmptrap_snmpuser_binding":<snmptrap_snmpuser_binding[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/snmptrap_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/snmptrap_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "snmptrap_binding": [ {

"trapclass":<String_value>,

"trapdestination":<String_value>,

"version":<String_value>,

"td":<Integer_value>,

"snmptrap_snmpuser_binding":<snmptrap_snmpuser_binding[]_value>

}]}
```

snmptrap_snmpuser_binding

Binding object showing the snmpuser that can be bound to snmptrap.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
td	<Integer>	Read-write	Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0. Minimum value = 0 Maximum value = 4094
username	<String>	Read-write	Name of the SNMP user that will send the SNMPv3 traps.
trapdestination	<String>	Read-write	IPv4 or the IPv6 address of the trap listener to which the Citrix ADC is to send SNMP trap messages. Minimum length = 1
trapclass	<String>	Read-write	Type of trap messages that the Citrix ADC sends to the trap listener: Generic or the enterprise-specific

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			messages defined in the MIB file. Possible values = generic, specific
securitylevel	<String>	Read-write	Security level of the SNMPv3 trap. Default value: authNoPriv, Possible values = noAuthNoPriv, authNoPriv, authPriv
version	<String>	Read-write	SNMP version, which determines the format of trap messages sent to the trap listener. This setting must match the setting on the trap listener. Otherwise, the listener drops the trap messages. Default value: V3 Possible values = V1, V2, V3
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

- ADD
- DELETE

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/snmptrap_snmpuser_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"snmptrap_snmpuser_binding":{

<b>"trapclass":<String_value>,

</b><b>"trapdestination":<String_value>,

</b>"td":<Integer_value>,

"version":<String_value>,

<b>"username":<String_value>,

</b>"securitylevel":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/snmptrap_snmpuser_binding/ trapclass_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ snmptrap_snmpuser_binding/ trapclass_value<String> ? **args= trapdestination:<String_value>, td: <Integer_value> ,version: <String_value> , username:<String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/snmptrap_snmpuser_binding **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/snmptrap_snmpuser_binding? **args=trapdestination:<String_value>,trapclass:<String_value>,td:<Integer_value>,version:<String_valu**

Use this query-parameter to get snmptrap_snmpuser_binding resources based on additional properties.

filter http:// <netscaler-ip-address> /nitro/v1/config/snmptrap_snmpuser_binding? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of snmptrap_snmpuser_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/snmptrap_snmpuser_binding? **pagesize=#no;pageno=#no**

Use this query-parameter to get the snmptrap_snmpuser_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "snmptrap_snmpuser_binding": [ {

"td":<Integer_value>,

"username":<String_value>,
```

```
"trapdestination":<String_value>,

"trapclass":<String_value>,

"securitylevel":<String_value>,

"version":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/snmptrap_snmpuser_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/snmptrap_snmpuser_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "snmptrap_snmpuser_binding": [ {

"td":<Integer_value>,
```

```
"username":<String_value>,

"trapdestination":<String_value>,

"trapclass":<String_value>,

"securitylevel":<String_value>,

"version":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/snmptrap_snmpuser_binding?
args=trapdestination:<String_value>,trapclass:<String_value>,td:<Integer_value>,version:<String_valu
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "snmptrap_snmpuser_binding": [ { "__count": "#no"} ] }
```

snmpuser

Configuration for SNMP user resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the SNMPv3 user. Can consist of 1 to 31 characters that include uppercase and lowercase letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore (_) characters. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose it in double or single quotation marks (for example, "my user" or 'my user'). Minimum length = 1
group	<String>	Read-write	Name of the configured SNMPv3 group to which to bind this SNMPv3 user. The access rights (bound SNMPv3 views) and security level set for

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			this group are assigned to this user. Minimum length = 1
authtype	<String>	Read-write	Authentication algorithm used by the Citrix ADC and the SNMPv3 user for authenticating the communication between them. You must specify the same authentication algorithm when you configure the SNMPv3 user in the SNMP manager. Possible values = MD5, SHA, SHA256, SHA512
authpasswd	<String>	Read-write	Plain-text pass phrase to be used by the authentication algorithm specified by the authType (Authentication Type) parameter. Can consist of 8 to 64 characters that include uppercase and lowercase letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore (_) characters.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			The following requirement applies only to the Citrix ADC CLI: If the pass phrase includes one or more spaces, enclose it in double or single quotation marks (for example, "my phrase" or 'my phrase'). Minimum length = 8
privtype	<String>	Read-write	Encryption algorithm used by the Citrix ADC and the SNMPv3 user for encrypting the communication between them. You must specify the same encryption algorithm when you configure the SNMPv3 user in the SNMP manager. Possible values = DES, AES, AES192, AES256
privpasswd	<String>	Read-write	Encryption key to be used by the encryption algorithm specified by the privType (Encryption Type) parameter. Can consist of 8 to

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			64 characters that include uppercase and lowercase letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore (_) characters. The following requirement applies only to the Citrix ADC CLI: If the key includes one or more spaces, enclose it in double or single quotation marks (for example, "my key" or 'my key'). Minimum length = 8
engineid	<String>	Read-only	The context engine ID of the user.
storagetype	<String>	Read-only	The storage type for this user. Possible values = volatile, nonVolatile
status	<String>	Read-only	The status of this user. Possible values = active

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/snmpuser **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"snmpuser":{

<b>"name":<String_value>,

</b><b>"group":<String_value>,

</b>"authtype":<String_value>,

"authpasswd":<String_value>,

"privtype":<String_value>,

"privpasswd":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/snmpuser/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/snmpuser **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"snmpuser":{

<b>"name":<String_value>,

</b>"group":<String_value>,

"authtype":<String_value>,

"authpasswd":<String_value>,

"privtype":<String_value>,

"privpasswd":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/snmpuser? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"snmpuser":{

<b>"name":<String_value>,

</b>"authtype":true,

"privtype":true,

"authpasswd":true,

"privpasswd":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/snmpuser **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/snmpuser? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/snmpuser? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of snmpuser resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/snmpuser? **view=summary**

Use this query-parameter to get the summary output of snmpuser resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/snmpuser? **pagesize=#no;pageno=#no**

Use this query-parameter to get the snmpuser resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "snmpuser": [ {

"name":<String_value>,

"group":<String_value>,

"authtype":<String_value>,

"privtype":<String_value>,

"engineid":<String_value>,

"storagetype":<String_value>,

"status":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/snmpuser/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/snmpuser/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/snmpuser/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of snmpuser resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "snmpuser": [ {

"name":<String_value>,

"group":<String_value>,

"authtype":<String_value>,
```

```
"privtype":<String_value>,

"engineid":<String_value>,

"storagetype":<String_value>,

"status":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/snmpuser? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "snmpuser": [ { "__count": "#no"} ] }
```

snmpview

Configuration for view resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the SNMPv3 view. Can consist of 1 to 31 characters that include uppercase and lowercase letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at sign (@), equals (=), colon (:), and underscore (_) characters. You should choose a name that helps identify the SNMPv3 view. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose it in double or single quotation marks (for example, "my view" or 'my view'). Minimum length = 1
subtree	<String>	Read-write	A particular branch (subtree) of the MIB tree that you want to associate with this SNMPv3 view. You must specify the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			subtree as an SNMP OID. Minimum length = 1
type	<String>	Read-write	Include or exclude the subtree, specified by the subtree parameter, in or from this view. This setting can be useful when you have included a subtree, such as A, in an SNMPv3 view and you want to exclude a specific subtree of A, such as B, from the SNMPv3 view. Possible values = included, excluded
storagetype	<String>	Read-only	The storage type for this view. Possible values = volatile, nonVolatile
status	<String>	Read-only	The status of this view. Possible values = active
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD

- DELETE
- UPDATE
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/snmpview **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"snmpview":{

<b>"name":<String_value>,

</b><b>"subtree":<String_value>,

</b><b>"type":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/snmpview/ name_value<String> **Query-parameters: args= subtree:<String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/snmpview **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"snmpview":{

<b>"name":<String_value>,

</b><b>"subtree":<String_value>,

</b><b>"type":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/snmpview **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/snmpview? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/snmpview? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of snmpview resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/snmpview? **view=summary**

Use this query-parameter to get the summary output of snmpview resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/snmpview? **pagesize=#no;pageno=#no**

Use this query-parameter to get the snmpview resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "snmpview": [ {

"name":<String_value>,

"subtree":<String_value>,

"type":<String_value>,

"storagetype":<String_value>,

"status":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/snmpview? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "snmpview": [ { "__count": "#no"} ] }
```

spillover

Spillover

Spillover policies and actions.

NAME	DESCRIPTION
spilloveraction	Configuration for Spillover action
spilloverpolicy	Configuration for Spillover policy
spilloverpolicy_binding	Binding object showing the resources that can be bound to spilloverpolicy
spilloverpolicy_csvserver_binding	Binding object showing the csvserver that can be bound to spilloverpolicy
spilloverpolicy_gslbvserver_binding	Binding object showing the gslbvserver that can be bound to spilloverpolicy
spilloverpolicy_lbvserver_binding	Binding object showing the lbvserver that can be bound to spilloverpolicy

spilloveraction

Configuration for Spillover action resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the spillover action.
action	<String>	Read-write	Spillover action. Currently only type SPILLOVER is supported. Possible values = SPILLOVER
newname	<String>	Read-write	New name for the spillover action. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Choose a name that can be correlated with the function that the action performs. The following requirement applies only to the Citrix ADC CLI:

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my action" or 'my action'). Minimum length = 1
builtin	<String[]>	Read-only	Flag to determine whether compression is default or not. Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL
feature	<String>	Read-only	The feature to be checked while applying this config.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET (ALL)
- GET
- COUNT

- RENAME

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/spilloveraction **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"spilloveraction":{

<b>"name":<String_value>,
```

```
</b><b>"action":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/spilloveraction/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

RENAME

URL: http:// <netscaler-ip-address> /nitro/v1/config/spilloveraction? **action=rename HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"spilloveraction":{

<b>"name":<String_value>,

</b><b>"newname":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/spilloveraction **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/spilloveraction? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/spilloveraction? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of spilloveraction resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/spilloveraction? **view=summary**

Use this query-parameter to get the summary output of spilloveraction resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/spilloveraction? **pagesize=#no;pageno=#no**

Use this query-parameter to get the spilloveraction resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "spilloveraction": [ {

"name":<String_value>,

"action":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/spilloveraction/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/spilloveraction/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/spilloveraction/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of spilloveraction resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "spilloveraction": [ {

"name":<String_value>,

"action":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/spilloveraction? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "spilloveraction": [ { "__count": "#no"} ] }
```

spilloverpolicy

Configuration for Spillover policy resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the spillover policy.
rule	<String>	Read-write	Expression to be used by the spillover policy.
action	<String>	Read-write	Action for the spillover policy. Action is created using add spillover action command.
comment	<String>	Read-write	Any comments that you might want to associate with the spillover policy.
newname	<String>	Read-write	New name for the spillover policy. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			hyphen (-) characters. Choose a name that reflects the function that the policy performs. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my policy" or 'my policy'). Minimum length = 1
hits	<Integer>	Read-only	The number of times the policy has been hit.
undefhits	<Integer>	Read-only	Number of policy UNDEF hits.
builtin	<String[]>	Read-only	Flag to determine if compression policy is builtin or not. Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
feature	<String>	Read-only	The feature to be checked while applying this config.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT
- RENAME

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/spilloverpolicy **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"spilloverpolicy":{

<b>"name":<String_value>,

</b><b>"rule":<String_value>,

</b><b>"action":<String_value>,

</b>"comment":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/spilloverpolicy/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/spilloverpolicy **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"spilloverpolicy":{

<b>"name":<String_value>,

</b>"rule":<String_value>,

"action":<String_value>,

"comment":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/spilloverpolicy? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"spilloverpolicy":{

<b>"name":<String_value>,

</b>"comment":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

RENAME

URL: http:// <netscaler-ip-address> /nitro/v1/config/spilloverpolicy? **action=rename HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"spilloverpolicy":{

<b>"name":<String_value>,

</b><b>"newname":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/spilloverpolicy **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/spilloverpolicy? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/spilloverpolicy? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of spilloverpolicy resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/spilloverpolicy? **view=summary**

Use this query-parameter to get the summary output of spilloverpolicy resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/spilloverpolicy? **pagesize=#no;pageno=#no**

Use this query-parameter to get the spilloverpolicy resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "spilloverpolicy": [ {

"name":<String_value>,

"rule":<String_value>,

"action":<String_value>,

"hits":<Integer_value>,

"undefhits":<Integer_value>,

"comment":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/spilloverpolicy/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/spilloverpolicy/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/spilloverpolicy/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of spilloverpolicy resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "spilloverpolicy": [ {

"name":<String_value>,

"rule":<String_value>,

"action":<String_value>,

"hits":<Integer_value>,

"undefhits":<Integer_value>,

"comment":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/spilloverpolicy? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "spilloverpolicy": [ { "__count": "#no"} ] }
```

spilloverpolicy_binding

Binding object which returns the resources bound to spilloverpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the spillover policy.
spilloverpolicy_lbvserver_binding	<spilloverpolicy_lbvserver_binding[]>	Read-only	lbvserver that can be bound to spilloverpolicy.
spilloverpolicy_gslbvserver_binding	<spilloverpolicy_gslbvserver_binding[]>	Read-only	gslbvserver that can be bound to spilloverpolicy.
spilloverpolicy_csvserver_binding	<spilloverpolicy_csvserver_binding[]>	Read-only	csvserver that can be bound to spilloverpolicy.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/spilloverpolicy_binding/ name_value<String>
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "spilloverpolicy_binding": [ {

"name":<String_value>,

"spilloverpolicy_gslbvserver_binding":<spilloverpolicy_gslbvserver_binding
[]_value>,

"spilloverpolicy_lbvserver_binding":<spilloverpolicy_lbvserver_binding[]_v
alue>,

"spilloverpolicy_csvserver_binding":<spilloverpolicy_csvserver_binding[]_v
alue>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/spilloverpolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/spilloverpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "spilloverpolicy_binding": [ {

"name":<String_value>,

"spilloverpolicy_gslbvserver_binding":<spilloverpolicy_gslbvserver_binding
[]_value>,

"spilloverpolicy_lbvserver_binding":<spilloverpolicy_lbvserver_binding[]_v
alue>,

"spilloverpolicy_csvserver_binding":<spilloverpolicy_csvserver_binding[]_v
alue>

}]}
```

spilloverpolicy_csvserver_binding

Binding object showing the csvserver that can be bound to spilloverpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the spillover policy.
boundto	<String>	Read-write	The name of the entity to which the policy is bound.
gotopriorityexpression	<String>	Read-only	Expression specifying the priority

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
labelname	<String>	Read-only	Name of the label to invoke if the current policy rule evaluates to TRUE.
activepolicy	<Integer>	Read-only	Indicates whether policy is bound or not.
priority	<Integer>	Read-only	Specifies the priority of the policy.
labeltype	<String>	Read-only	Type of policy label invocation. Possible values = reqvserver, resvserver, policylabel
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/spilloverpolicy_csvserver_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ spilloverpolicy_csvserver_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of spilloverpolicy_csvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/spilloverpolicy_csvserver_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the spilloverpolicy_csvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "spilloverpolicy_csvserver_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"gotopriorityexpression":<String_value>,

"labelname":<String_value>,

"activepolicy":<Integer_value>,

"priority":<Integer_value>,

"labeltype":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/spilloverpolicy_csvserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/spilloverpolicy_csvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "spilloverpolicy_csvserver_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"gotopriorityexpression":<String_value>,

"labelname":<String_value>,

"activepolicy":<Integer_value>,

"priority":<Integer_value>,

"labeltype":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/spilloverpolicy_csvserver_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"spilloverpolicy_csvserver_binding": [ { "__count": "#no"} ] }
```

spilloverpolicy_gslbvserver_binding

Binding object showing the gslbvserver that can be bound to spilloverpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the spillover policy.
boundto	<String>	Read-write	The name of the entity to which the policy is bound.
activepolicy	<Integer>	Read-only	Indicates whether policy is bound or not.
labeltype	<String>	Read-only	Type of policy label invocation. Possible values = reqvserver, resvserver, policylabel

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
priority	<Integer>	Read-only	Specifies the priority of the policy.
labelname	<String>	Read-only	Name of the label to invoke if the current policy rule evaluates to TRUE.
gotopriorityexpression	<String>	Read-only	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of

creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/spilloverpolicy_gslbvserver_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ spilloverpolicy_gslbvserver_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of spilloverpolicy_gslbvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/spilloverpolicy_gslbvserver_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the spilloverpolicy_gslbvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "spilloverpolicy_gslbvserver_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"activepolicy":<Integer_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"labelname":<String_value>,

"gotopriorityexpression":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/spilloverpolicy_gslbvserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/spilloverpolicy_gslbvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "spilloverpolicy_gslbvserver_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"activepolicy":<Integer_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"labelname":<String_value>,

"gotopriorityexpression":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/spilloverpolicy_gslbvserver_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"spilloverpolicy_gslbvserver_binding": [ { "__count": "#no"} ] }
```

spilloverpolicy_lbvserver_binding

Binding object showing the lbvserver that can be bound to spilloverpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
boundto	<String>	Read-write	The name of the entity to which the policy is bound.
name	<String>	Read-write	Name of the spillover policy.
priority	<Integer>	Read-only	Specifies the priority of the policy.
labeltype	<String>	Read-only	Type of policy label invocation. Possible values = reqvserver, resvserver, policylabel
activepolicy	<Integer>	Read-only	Indicates whether policy is bound or not.
gotopriorityexpression	<String>	Read-only	Expression specifying the priority of the next policy which will get

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			evaluated if the current policy rule evaluates to TRUE.
labelname	<String>	Read-only	Name of the label to invoke if the current policy rule evaluates to TRUE.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/spilloverpolicy_lbvserver_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ spilloverpolicy_lbvserver_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of spilloverpolicy_lbvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/spilloverpolicy_lbvserver_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the spilloverpolicy_lbvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "spilloverpolicy_lbvserver_binding": [ {

"boundto":<String_value>,

"name":<String_value>,
```

```
"priority":<Integer_value>,

"labeltype":<String_value>,

"activepolicy":<Integer_value>,

"gotopriorityexpression":<String_value>,

"labelname":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/spilloverpolicy_lbvserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/spilloverpolicy_lbvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "spilloverpolicy_lbvserver_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"priority":<Integer_value>,

"labeltype":<String_value>,

"activepolicy":<Integer_value>,

"gotopriorityexpression":<String_value>,

"labelname":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/spilloverpolicy_lbvserver_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"spilloverpolicy_lbvserver_binding": [ { "__count": "#no"} ] }
```

ssl

SSL

SSL Configuration

NAME	DESCRIPTION
sslaction	Configuration for SSL action
sslcacertbundle	Configuration for CA certbundle
sslcacertbundle_binding	Binding object showing the resources that can be bound to sslcacertbundle
sslcacertbundle_intermediatecacertlist_binding	Binding object showing the intermediatecacertlist that can be bound to sslcacertbundle
sslcacertgroup	Configuration for Group of CA certificate-key pairs
sslcacertgroup_binding	Binding object showing the resources that can be bound to sslcacertgroup
sslcacertgroup_sslcertkey_binding	Binding object showing the sslcertkey that can be bound to sslcacertgroup
sslcert	Configuration for cerificate
sslcertbundle	Configuration for Imported Certbundle
sslcertchain	Configuration for CERT Chain
sslcertchain_binding	Binding object showing the resources that can be bound to sslcertchain
sslcertchain_sslcertkey_binding	Binding object showing the sslcertkey that can be bound to sslcertchain
sslcertfile	Configuration for Imported Certfile

NAME	DESCRIPTION
sslcertificatechain	Configuration for linked certificate
sslcertkey	Configuration for certificate key
sslcertkey_binding	Binding object showing the resources that can be bound to sslcertkey
sslcertkey_crldistribution_binding	Binding object showing the crldistribution that can be bound to sslcertkey
sslcertkey_service_binding	Binding object showing the service that can be bound to sslcertkey
sslcertkey_sslocspresponder_binding	Binding object showing the sslocspresponder that can be bound to sslcertkey
sslcertkey_sslprofile_binding	Binding object showing the sslprofile that can be bound to sslcertkey
sslcertkey_sslvserver_binding	Binding object showing the sslvserver that can be bound to sslcertkey
sslcertkeybundle	Configuration for certkey bundle
sslcertkeybundle_binding	Binding object showing the resources that can be bound to sslcertkeybundle
sslcertkeybundle_intermediatecertlinks_binding	Binding object showing the intermediatecertlinks that can be bound to sslcertkeybundle
sslcertkeybundle_sslvserver_binding	Binding object showing the sslvserver that can be bound to sslcertkeybundle
sslcertlink	Configuration for linked certificate
sslcertreq	Configuration for certificate request

NAME	DESCRIPTION
sslcipher	Configuration for cipher
sslcipher_binding	Binding object showing the resources that can be bound to sslcipher
sslcipher_individualcipher_binding	Binding object showing the individualcipher that can be bound to sslcipher
sslcipher_service_binding	Binding object showing the service that can be bound to sslcipher
sslcipher_servicegroup_binding	Binding object showing the servicegroup that can be bound to sslcipher
sslcipher_sslciphersuite_binding	Binding object showing the sslciphersuite that can be bound to sslcipher
sslcipher_sslprofile_binding	Binding object showing the sslprofile that can be bound to sslcipher
sslcipher_sslvserver_binding	Binding object showing the sslvserver that can be bound to sslcipher
sslciphersuite	Configuration for ciphersuite
sslcrl	Configuration for Certificate Revocation List
sslcrl_binding	Binding object showing the resources that can be bound to sslcrl
sslcrl_serialnumber_binding	Binding object showing the serialnumber that can be bound to sslcrl
sslcrlfile	Configuration for Imported crl files
ssldefaultprofile	
ssldhfile	Configuration for dh imported file

NAME	DESCRIPTION
ssldhparam	Configuration for dh Parameter
ssldtlsprofile	Configuration for DTLS profile
ssldynamicclientcertcache	Configuration for Dynamic Client Certificate Cache
sslecdsakey	Configuration for ecdsa key
sslechconfig	Configuration for ech config
sslfips	Configuration for fips
sslfipskey	Configuration for FIPS key
sslfipssimsource	Configuration for FIPsSIM source
sslfipssimtarget	Configuration for FIPS SIM Target
sslglobal_binding	Binding object showing the resources that can be bound to sslglobal
sslglobal_sslpolicy_binding	Binding object showing the sslpolicy that can be bound to sslglobal
sslhpkekey	Configuration for HPKE key
sslhsmkey	Configuration for HSM key
sslkeyfile	Configuration for Imported ssl key files
ssllogprofile	Configuration for SSL logging Profile
sslocspresponder	Configuration for OCSP responser
sslparameter	Configuration for SSL parameter
sslpkcs12	Configuration for pkcs12

NAME	DESCRIPTION
sslpkcs8	Configuration for pkcs8
sslpolicy	Configuration for SSL policy
sslpolicy_binding	Binding object showing the resources that can be bound to sslpolicy
sslpolicy_csvserver_binding	Binding object showing the csvserver that can be bound to sslpolicy
sslpolicy_lbvserver_binding	Binding object showing the lbvserver that can be bound to sslpolicy
sslpolicy_sslglobal_binding	Binding object showing the sslglobal that can be bound to sslpolicy
sslpolicy_sslpolicylabel_binding	Binding object showing the sslpolicylabel that can be bound to sslpolicy
sslpolicy_sslservice_binding	Binding object showing the sslservice that can be bound to sslpolicy
sslpolicy_sslvserver_binding	Binding object showing the sslvserver that can be bound to sslpolicy
sslpolicylabel	Configuration for SSL policy label
sslpolicylabel_binding	Binding object showing the resources that can be bound to sslpolicylabel
sslpolicylabel_sslpolicy_binding	Binding object showing the sslpolicy that can be bound to sslpolicylabel
sslprofile	Configuration for SSL profile
sslprofile_binding	Binding object showing the resources that can be bound to sslprofile

NAME	DESCRIPTION
sslprofile_ecccurve_binding	Binding object showing the ecccurve that can be bound to sslprofile
sslprofile_sslcertkey_binding	Binding object showing the sslcertkey that can be bound to sslprofile
sslprofile_sslcipher_binding	Binding object showing the sslcipher that can be bound to sslprofile
sslprofile_sslciphersuite_binding	Binding object showing the sslciphersuite that can be bound to sslprofile
sslprofile_sslechconfig_binding	Binding object showing the sslechconfig that can be bound to sslprofile
sslprofile_sslvserver_binding	Binding object showing the sslvserver that can be bound to sslprofile
sslrsakey	Configuration for RSA key
sslservice	Configuration for SSL service
sslservice_binding	Binding object showing the resources that can be bound to sslservice
sslservice_ecccurve_binding	Binding object showing the ecccurve that can be bound to sslservice
sslservice_sslcacertbundle_binding	Binding object showing the sslcacertbundle that can be bound to sslservice
sslservice_sslcertkey_binding	Binding object showing the sslcertkey that can be bound to sslservice
sslservice_sslcipher_binding	Binding object showing the sslcipher that can be bound to sslservice

NAME	DESCRIPTION
sslservice_sslciphersuite_binding	Binding object showing the sslciphersuite that can be bound to sslservice
sslservice_sslpolicy_binding	Binding object showing the sslpolicy that can be bound to sslservice
sslservicegroup	Configuration for SSL service group
sslservicegroup_binding	Binding object showing the resources that can be bound to sslservicegroup
sslservicegroup_ecccurve_binding	Binding object showing the ecccurve that can be bound to sslservicegroup
sslservicegroup_sslcacertbundle_binding	Binding object showing the sslcacertbundle that can be bound to sslservicegroup
sslservicegroup_sslcertkey_binding	Binding object showing the sslcertkey that can be bound to sslservicegroup
sslservicegroup_sslcipher_binding	Binding object showing the sslcipher that can be bound to sslservicegroup
sslservicegroup_sslciphersuite_binding	Binding object showing the sslciphersuite that can be bound to sslservicegroup
sslvserver	Configuration for SSL virtual server
sslvserver_binding	Binding object showing the resources that can be bound to sslvserver
sslvserver_ecccurve_binding	Binding object showing the ecccurve that can be bound to sslvserver
sslvserver_hashicorp_binding	Binding object showing the hashicorp that can be bound to sslvserver

NAME	DESCRIPTION
sslvserver_sslcacertbundle_binding	Binding object showing the sslcacertbundle that can be bound to sslvserver
sslvserver_sslcertkey_binding	Binding object showing the sslcertkey that can be bound to sslvserver
sslvserver_sslcertkeybundle_binding	Binding object showing the sslcertkeybundle that can be bound to sslvserver
sslvserver_sslcipher_binding	Binding object showing the sslcipher that can be bound to sslvserver
sslvserver_sslciphersuite_binding	Binding object showing the sslciphersuite that can be bound to sslvserver
sslvserver_sslpolicy_binding	Binding object showing the sslpolicy that can be bound to sslvserver
sslwrapkey	Configuration for WRAP key
sslzerotouchparam	Configuration for Zerotouch params

sslaction

Configuration for SSL action resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the SSL action. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the action is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my action" or 'my action'). Minimum length = 1
clientauth	<String>	Read-write	Perform client certificate authentication. Possible values = DOCLIENTAUTH, NOCLIENTAUTH
clientcertverification	<String>	Read-write	Client certificate verification is mandatory or optional. Default value: Mandatory

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = Mandatory, Optional
ssllogprofile	<String>	Read-write	The name of the ssllogprofile. Minimum length = 1 Maximum length = 127
clientcert	<String>	Read-write	Insert the entire client certificate into the HTTP header of the request being sent to the web server. The certificate is inserted in ASCII (PEM) format. Possible values = ENABLED, DISABLED
certheader	<String>	Read-write	Name of the header into which to insert the client certificate.
clientcertserialnumber	<String>	Read-write	Insert the entire client serial number into the HTTP header of the request being sent to the web server. Possible values = ENABLED, DISABLED
certserialheader	<String>	Read-write	Name of the header into which to insert

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			the client serial number.
clientcertsubject	<String>	Read-write	Insert the client certificate subject, also known as the distinguished name (DN), into the HTTP header of the request being sent to the web server. Possible values = ENABLED, DISABLED
certsubjectheader	<String>	Read-write	Name of the header into which to insert the client certificate subject.
clientcerthash	<String>	Read-write	Insert the certificate's signature into the HTTP header of the request being sent to the web server. The signature is the value extracted directly from the X.509 certificate signature field. All X.509 certificates contain a signature field. Possible values = ENABLED, DISABLED
certhashheader	<String>	Read-write	Name of the header into which to insert the client certificate signature (hash).

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
clientcertfingerprint	<String>	Read-write	Insert the certificate's fingerprint into the HTTP header of the request being sent to the web server. The fingerprint is derived by computing the specified hash value (SHA256, for example) of the DER-encoding of the client certificate. Possible values = ENABLED, DISABLED
certfingerprintheader	<String>	Read-write	Name of the header into which to insert the client certificate fingerprint.
certfingerprintdigest	<String>	Read-write	Digest algorithm used to compute the fingerprint of the client certificate. Possible values = SHA1, SHA224, SHA256, SHA384, SHA512
clientcertissuer	<String>	Read-write	Insert the certificate issuer details into the HTTP header of the request being sent to the web server. Possible values = ENABLED, DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
certissuerheader	<String>	Read-write	Name of the header into which to insert the client certificate issuer details.
sessionid	<String>	Read-write	Insert the SSL session ID into the HTTP header of the request being sent to the web server. Every SSL connection that the client and the Citrix ADC share has a unique ID that identifies the specific connection. Possible values = ENABLED, DISABLED
sessionidheader	<String>	Read-write	Name of the header into which to insert the Session ID.
cipher	<String>	Read-write	Insert the cipher suite that the client and the Citrix ADC negotiated for the SSL session into the HTTP header of the request being sent to the web server. The appliance inserts the cipher-suite name, SSL protocol, export or non-export string, and cipher strength bit, depending on the type of browser connecting to the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			SSL virtual server or service (for example, Cipher-Suite: RC4-MD5 SSLv3 Non-Export 128-bit). Possible values = ENABLED, DISABLED
cipherheader	<String>	Read-write	Name of the header into which to insert the name of the cipher suite.
clientcertnotbefore	<String>	Read-write	Insert the date from which the certificate is valid into the HTTP header of the request being sent to the web server. Every certificate is configured with the date and time from which it is valid. Possible values = ENABLED, DISABLED
certnotbeforeheader	<String>	Read-write	Name of the header into which to insert the date and time from which the certificate is valid.
clientcertnotafter	<String>	Read-write	Insert the date of expiry of the certificate into the HTTP header of the request being sent to the web server. Every certificate is

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			configured with the date and time at which the certificate expires. Possible values = ENABLED, DISABLED
certnotafterheader	<String>	Read-write	Name of the header into which to insert the certificate's expiry date.
owasupport	<String>	Read-write	If the appliance is in front of an Outlook Web Access (OWA) server, insert a special header field, FRONT-END-HTTPS: ON, into the HTTP requests going to the OWA server. This header communicates to the server that the transaction is HTTPS and not HTTP. Possible values = ENABLED, DISABLED
forward	<String>	Read-write	This action takes an argument a vserver name, to this vserver one will be able to forward all the packets. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum length = 127
cacertgrpname	<String>	Read-write	This action will allow to pick CA(s) from the specific CA group, to verify the client certificate. Minimum length = 1 Maximum length = 31
ocspstapling	<String>	Read-write	This option is used to enable ocspStapling parameter for the SSL connection. Possible values = ENABLED, DISABLED
ocspcertvalidation	<String>	Read-write	This option is used to check the revocation status of client/server certificate in SSL handshake using OCSP. Possible values = DISABLE, OPTIONAL, MANDATORY
ocspcache	<String>	Read-write	Enable cache of OCSP response. Caching of response received from the OCSP responder enables faster response to the client and reduces

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			the load on the OCSP responder. Default value: DISABLED Possible values = ENABLED, DISABLED
inhandshakeclientauth	<String>	Read-write	This option dynamically enables client authentication for the specific SSL connection based on policy evaluation performed during ClientHello handshake message processing. It overrides the clientAuth setting configured on the SSL virtual server or the SSL frontend profile. Possible values = ENABLED, DISABLED
inhandshakeclientcertverification	<String>	Read-write	Specifies the type of client authentication and is applicable only when inHandshakeClientAuth is ENABLED. If set to MANDATORY, the appliance terminates the SSL handshake when the client fails to present

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			a valid certificate. If set to OPTIONAL, the appliance requests a client certificate but continues the SSL transaction even if the certificate is missing or invalid. Default value is MANDATORY. Possible values = Mandatory, Optional
alpnhttp2	<String>	Read-write	This option is used to enable or disable the HTTP/2 application protocol based on policy evaluation performed during ClientHello handshake message processing. Possible values = ENABLED, DISABLED
hits	<Integer>	Read-only	The number of times the action has been taken.
undefhits	<Integer>	Read-only	The number of times the action resulted in UNDEF.
referencecount	<Integer>	Read-only	The number of references to the action.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
description	<String>	Read-only	Description of the action.
builtin	<String[]>	Read-only	Flag to determine whether ssl action is built-in or not. Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL
feature	<String>	Read-only	The feature to be checked while applying this config.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslaction **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"sslaction":{

<b>"name":<String_value>,

</b>"clientauth":<String_value>,

"clientcertverification":<String_value>,

"ssllogprofile":<String_value>,

"clientcert":<String_value>,

"certheader":<String_value>,
```

```
"clientcertserialnumber":<String_value>,

"certserialheader":<String_value>,

"clientcertsubject":<String_value>,

"certsubjectheader":<String_value>,

"clientcerthash":<String_value>,

"certhashheader":<String_value>,

"clientcertfingerprint":<String_value>,

"certfingerprintheader":<String_value>,

"certfingerprintdigest":<String_value>,

"clientcertissuer":<String_value>,

"certissuerheader":<String_value>,

"sessionid":<String_value>,

"sessionidheader":<String_value>,

"cipher":<String_value>,

"cipherheader":<String_value>,

"clientcertnotbefore":<String_value>,

"certnotbeforeheader":<String_value>,

"clientcertnotafter":<String_value>,

"certnotafterheader":<String_value>,

"owasupport":<String_value>,

"forward":<String_value>,

"cacertgrpname":<String_value>,
```

```
"ocspstapling":<String_value>,

"ocspcertvalidation":<String_value>,

"ocspcache":<String_value>,

"inhandshakeclientauth":<String_value>,

"inhandshakeclientcertverification":<String_value>,

"alpnhttp2":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslaction/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslaction **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/sslaction? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/sslaction? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of sslaction resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/sslaction? **view=summary**

Use this query-parameter to get the summary output of sslaction resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/sslaction? **pagesize=#no;pageno=#no**

Use this query-parameter to get the sslaction resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "sslaction": [ {

"name":<String_value>,

"clientauth":<String_value>,

"clientcertverification":<String_value>,

"clientcert":<String_value>,

"certheader":<String_value>,
```

```
"clientcertserialnumber":<String_value>,

"certserialheader":<String_value>,

"clientcertsubject":<String_value>,

"certsubjectheader":<String_value>,

"clientcerthash":<String_value>,

"certhashheader":<String_value>,

"clientcertfingerprint":<String_value>,

"certfingerprintheader":<String_value>,

"certfingerprintdigest":<String_value>,

"clientcertissuer":<String_value>,

"certissuerheader":<String_value>,

"sessionid":<String_value>,

"sessionidheader":<String_value>,

"cipher":<String_value>,

"cipherheader":<String_value>,

"owasupport":<String_value>,

"forward":<String_value>,

"cacertgrpname":<String_value>,

"clientcertnotbefore":<String_value>,

"certnotbeforeheader":<String_value>,

"clientcertnotafter":<String_value>,

"certnotafterheader":<String_value>,
```

```
"ocspcertvalidation":<String_value>,

"ocspstapling":<String_value>,

"ocspcache":<String_value>,

"inhandshakeclientauth":<String_value>,

"inhandshakeclientcertverification":<String_value>,

"alpnhttp2":<String_value>,

"hits":<Integer_value>,

"undefhits":<Integer_value>,

"referencecount":<Integer_value>,

"description":<String_value>,

"ssllogprofile":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslaction/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/sslaction/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/sslaction/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of sslaction resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslaction": [ {

"name":<String_value>,

"clientauth":<String_value>,

"clientcertverification":<String_value>,

"clientcert":<String_value>,

"certheader":<String_value>,

"clientcertserialnumber":<String_value>,

"certserialheader":<String_value>,

"clientcertsubject":<String_value>,

"certsubjectheader":<String_value>,
```

```
"clientcerthash":<String_value>,

"certhashheader":<String_value>,

"clientcertfingerprint":<String_value>,

"certfingerprintheader":<String_value>,

"certfingerprintdigest":<String_value>,

"clientcertissuer":<String_value>,

"certissuerheader":<String_value>,

"sessionid":<String_value>,

"sessionidheader":<String_value>,

"cipher":<String_value>,

"cipherheader":<String_value>,

"owasupport":<String_value>,

"forward":<String_value>,

"cacertgrpname":<String_value>,

"clientcertnotbefore":<String_value>,

"certnotbeforeheader":<String_value>,

"clientcertnotafter":<String_value>,

"certnotafterheader":<String_value>,

"ocspcertvalidation":<String_value>,

"ocspstapling":<String_value>,

"ocspcache":<String_value>,

"inhandshakeclientauth":<String_value>,
```

```
"inhandshakeclientcertverification":<String_value>,

"alpnhttp2":<String_value>,

"hits":<Integer_value>,

"undefhits":<Integer_value>,

"referencecount":<Integer_value>,

"description":<String_value>,

"ssllogprofile":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslaction? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "sslaction": [ { "__count": "#no"} ] }
```

sslcacertbundle

Configuration for CA certbundle resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
cacertbundlename	<String>	Read-write	Name given to the CA certbundle. The name will be used for bind/unbind/update operations. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my file" or 'my file'). Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum length = 127
bundlefile	<String>	Read-write	Name of and, optionally, path to the X509 CA certificate bundle file that is used to form cacertbundle entity. The CA certificate bundle file should be present on the appliance's hard-disk drive or solid-state drive. /nsconfig/ssl/ is the default path. The CA certificate bundle file consists of list of certificates. Minimum length = 1
servername	<String>	Read-only	Vserver/Service/ Servicegroup name to which the cacertbundle is bound.
cacertbundledigest	<String>	Read-only	Stores the digest of a CA certificate bundle file.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE

- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcacertbundle **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"sslcacertbundle":{

<b>"cacertbundlename":<String_value>,

</b><b>"bundlefile":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcacertbundle/ cacertbundlename_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcacertbundle **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/sslcacertbundle? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/sslcacertbundle? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of sslcacertbundle resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/sslcacertbundle? **view=summary**

Use this query-parameter to get the summary output of sslcacertbundle resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/sslcacertbundle? **pagesize=#no;pageno=#no**

Use this query-parameter to get the sslcacertbundle resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "sslcacertbundle": [ {

"cacertbundlename":<String_value>,

"bundlefile":<String_value>,

"servername":<String_value>,

"cacertbundledigest":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcacertbundle/ cacertbundlename_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/sslcacertbundle/ cacertbundlename_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/sslcacertbundle/ cacertbundlename_value<String> ? **view=summary**

Use this query-parameter to get the summary output of sslcacertbundle resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslcacertbundle": [ {

"cacertbundlename":<String_value>,

"bundlefile":<String_value>,

"servername":<String_value>,

"cacertbundledigest":<String_value>,
```

```
"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcacertbundle? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "sslcacertbundle": [ { "__count": "#no"} ] }
```

sslcacertbundle_binding

Binding object which returns the resources bound to sslcacertbundle.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
cacertbundlename	<String>	Read-write	Name given to the CA certbundle. The name will be used for bind/unbind/update

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			operations. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my file" or 'my file'). Minimum length = 1 Maximum length = 127
sslcacertbundle_intermediatecacertlist_binding	<sslcacertbundle_intermediatecacertlist_binding[]>	Read-only	intermediatecacertlist that can be bound to sslcacertbundle.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcacertbundle_binding/cacertbundlename_value<String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "sslcacertbundle_binding": [ {

"cacertbundlename":<String_value>,

"sslcacertbundle_intermediatecacertlist_binding":<sslcacertbundle_intermed
iatecacertlist_binding[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcacertbundle_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/sslcacertbundle_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "sslcacertbundle_binding": [ {

"cacertbundlename":<String_value>,

"sslcacertbundle_intermediatecacertlist_binding":<sslcacertbundle_intermed
```

```
iatecacertlist_binding[]_value>

}]}
```

sslcacertbundle_intermediatecacertlist_binding

Binding object showing the intermediatecacertlist that can be bound to sslcacertbundle.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
subject	<String>	Read-write	Subject name.
cacertbundlename	<String>	Read-write	Name given to the CA certbundle. The name will be used for bind/unbind/update operations. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			example, "my file" or 'my file'). Minimum length = 1 Maximum length = 127
clientcertnotafter	<String>	Read-only	Not-After date.
status	<String>	Read-only	Status of the certificate. Possible values = Valid, Not yet valid, Expired
clientcertnotbefore	<String>	Read-only	Not-Before date.
issuer	<String>	Read-only	Issuer name.
daystoexpiration	<Integer>	Read-only	Days remaining for the certificate to expire.
sandns	<String>	Read-only	Subject Alternative Name (SAN) is an extension to X.509 that allows various values to be associated with a security certificate using a subjectAltName field. These values are called "Subject Alternative Names" (SAN). This field is for DNS names.
publickeysize	<Integer>	Read-only	Size of the public key.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
sanipadd	<String>	Read-only	Subject Alternative Name (SAN) is an extension to X.509 that allows various values to be associated with a security certificate using a subjectAltName field. These values are called "Subject Alternative Names" (SAN). This field is for IP address.
signaturealg	<String>	Read-only	Signature algorithm.
serial	<String>	Read-only	Serial number.
publickey	<String>	Read-only	Public key algorithm.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcacertbundle_intermediatecacertlist_binding/ cacertbundlename_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/sslcacertbundle_intermediatecacertlist_binding/ cacertbundlename_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of sslcacertbundle_intermediatecacertlist_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ sslcacertbundle_intermediatecacertlist_binding/ cacertbundlename_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the sslcacertbundle_intermediatecacertlist_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslcacertbundle_intermediatecacertlist_binding": [ {

"subject":<String_value>,

"cacertbundlename":<String_value>,

"clientcertnotafter":<String_value>,

"status":<String_value>,

"clientcertnotbefore":<String_value>,

"issuer":<String_value>,

"daystoexpiration":<Integer_value>,

"sandns":<String_value>,

"publickeysize":<Integer_value>,

"sanipadd":<String_value>,

"signaturealg":<String_value>,

"serial":<String_value>,

"publickey":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcacertbundle_intermediatecacertlist_binding
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/sslcacertbundle_intermediatecacertlist_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslcacertbundle_intermediatecacertlist_binding": [ {

"subject":<String_value>,

"cacertbundlename":<String_value>,

"clientcertnotafter":<String_value>,

"status":<String_value>,

"clientcertnotbefore":<String_value>,

"issuer":<String_value>,

"daystoexpiration":<Integer_value>,
```

```
"sandns":<String_value>,

"publickeysize":<Integer_value>,

"sanipadd":<String_value>,

"signaturealg":<String_value>,

"serial":<String_value>,

"publickey":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcacertbundle_intermediatecacertlist_binding/cacertbundlename_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"sslcacertbundle_intermediatecacertlist_binding": [ { "__count":
"#no"} ] }
```

sslcacertgroup

Configuration for Group of CA certificate-key pairs resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
cacertgroupname	<String>	Read-write	Name given to the CA certificate group. The name will be used to add the CA certificates to the group. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my file" or 'my file'). Minimum length = 1 Maximum length = 31

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
cacertgroupreferences	<Integer>	Read-only	Count for ssl actions referring to this ca certificate group.
ocspcheck	<String>	Read-only	The state of the OCSP check parameter. (Mandatory/ Optional). Possible values = Mandatory, Optional
crlcheck	<String>	Read-only	The state of the CRL check parameter. (Mandatory/ Optional). Possible values = Mandatory, Optional
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcacertgroup **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"sslcacertgroup":{

<b>"cacertgroupname":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcacertgroup/ cacertgroupname_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcacertgroup **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/sslcacertgroup? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/sslcacertgroup? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of sslcacertgroup resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/sslcacertgroup? **view=summary**

Use this query-parameter to get the summary output of sslcacertgroup resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/sslcacertgroup? **pagesize=#no;pageno=#no**

Use this query-parameter to get the sslcacertgroup resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "sslcacertgroup": [ {

"cacertgroupname":<String_value>,

"cacertgroupreferences":<Integer_value>,

"ocspcheck":<String_value>,

"crlcheck":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcacertgroup/ cacertgroupname_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/ config/sslcacertgroup/ cacertgroupname_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/sslcacertgroup/ cacertgroupname_value<String> ? **view=summary**

Use this query-parameter to get the summary output of sslcacertgroup resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslcacertgroup": [ {

"cacertgroupname":<String_value>,

"cacertgroupreferences":<Integer_value>,

"ocspcheck":<String_value>,

"crlcheck":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcacertgroup? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "sslcacertgroup": [ { "__count": "#no"} ] }
```

sslcacertgroup_binding

Binding object which returns the resources bound to sslcacertgroup.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
cacertgroupname	<String>	Read-write	Name of the CA certificate group for which to show detailed information. Minimum length = 1 Maximum length = 31
sslcacertgroup_sslcertkey_binding	<sslcacertgroup_sslcertkey_binding[]>	Read-only	sslcertkey that can be bound to sslcacertgroup.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcacertgroup_binding/cacertgroupname_value<String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "sslcacertgroup_binding": [ {

"cacertgroupname":<String_value>,

"sslcacertgroup_sslcertkey_binding":<sslcacertgroup_sslcertkey_binding[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcacertgroup_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/sslcacertgroup_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "sslcacertgroup_binding": [ {

"cacertgroupname":<String_value>,
```

```
"sslcacertgroup_sslcertkey_binding":<sslcacertgroup_sslcertkey_binding[]_value>

}]}
```

sslcacertgroup_sslcertkey_binding

Binding object showing the sslcertkey that can be bound to sslcacertgroup.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ocspcheck	<String>	Read-write	The state of the OCSP check parameter. (Mandatory/ Optional). Possible values = Mandatory, Optional
certkeyname	<String>	Read-write	Name for the certkey added to the Citrix ADC. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the certificate-key pair is created.The following

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my cert" or 'my cert'). Minimum length = 1 Maximum length = 63
crlcheck	<String>	Read-write	The state of the CRL check parameter. (Mandatory/ Optional). Possible values = Mandatory, Optional
cacertgroupname	<String>	Read-write	Name given to the CA certificate group. The name will be used to add the CA certificates to the group. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. The following

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my file" or 'my file'). Minimum length = 1 Maximum length = 31
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of

creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/sslcacertgroup_sslcertkey_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"sslcacertgroup_sslcertkey_binding":{

<b>"cacertgroupname":<String_value>,

</b><b>"certkeyname":<String_value>,

</b>"crlcheck":<String_value>,

"ocspcheck":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcacertgroup_sslcertkey_binding/ cacertgroupname_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/ config/sslcacertgroup_sslcertkey_binding/ cacertgroupname_value<String> ? **args= certkeyname:<String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcacertgroup_sslcertkey_binding/ cacertgroupname_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/ config/sslcacertgroup_sslcertkey_binding/ cacertgroupname_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of sslcacertgroup_sslcertkey_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/sslcacertgroup_sslcertkey_binding/ cacertgroupname_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the sslcacertgroup_sslcertkey_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslcacertgroup_sslcertkey_binding": [ {

"ocspcheck":<String_value>,

"certkeyname":<String_value>,

"crlcheck":<String_value>,

"cacertgroupname":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcacertgroup_sslcertkey_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/sslcacertgroup_sslcertkey_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslcacertgroup_sslcertkey_binding": [ {

"ocspcheck":<String_value>,

"certkeyname":<String_value>,

"crlcheck":<String_value>,

"cacertgroupname":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcacertgroup_sslcertkey_binding/ cacertgroupname_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"sslcacertgroup_sslcertkey_binding": [ { "__count": "#no"} ] }
```

sslcert

Configuration for cerificate resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
certfile	<String>	Read-write	Name for and, optionally, path to the generated certificate file. /nsconfig/ssl/ is the default path. Maximum length = 63
reqfile	<String>	Read-write	Name for and, optionally, path to the certificate-signing request (CSR). /nsconfig/ssl/ is the default path. Maximum length = 63
certtype	<String>	Read-write	Type of certificate to generate. Specify one of the following: * ROOT_CERT - Self-signed Root-CA certificate. You must specify the key file name. The generated Root-CA certificate can be used for signing end-user client or server certificates or to create

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Intermediate-CA certificates. * INTM_CERT - Intermediate-CA certificate. * CLNT_CERT - End-user client certificate used for client authentication. * SRVR_CERT - SSL server certificate used on SSL servers for end-to-end encryption. Possible values = ROOT_CERT, INTM_CERT, CLNT_CERT, SRVR_CERT
keyfile	<String>	Read-write	Name for and, optionally, path to the private key. You can either use an existing RSA or DSA key that you own or create a new private key on the Citrix ADC. This file is required only when creating a self-signed Root-CA certificate. The key file is stored in the /

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			nsconfig/ssl directory by default. If the input key specified is an encrypted key, you are prompted to enter the PEM pass phrase that was used for encrypting the key. Maximum length = 63
keyform	<String>	Read-write	Format in which the key is stored on the appliance. Default value: PEM Possible values = DER, PEM
pempassphrase	<String>	Read-write	. Minimum length = 1 Maximum length = 31
days	<Integer>	Read-write	Number of days for which the certificate will be valid, beginning with the time and day (system time) of creation. Default value: 365 Minimum value = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum value = 3650
subjectaltname	<String>	Read-write	Subject Alternative Name (SAN) is an extension to X.509 that allows various values to be associated with a security certificate using a subjectAltName field. These values are called "Subject Alternative Names" (SAN). Names include: 1. Email addresses 2. IP addresses 3. URIs 4. DNS names (This is usually also provided as the Common Name RDN within the Subject field of the main certificate.) 5. directory names (alternative Distinguished Names to that given in the Subject). Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
certform	<String>	Read-write	Format in which the certificate is stored on the appliance. Default value: PEM Possible values = DER, PEM
cacert	<String>	Read-write	Name of the CA certificate file that issues and signs the Intermediate-CA certificate or the end-user client and server certificates. Maximum length = 63
cacertform	<String>	Read-write	Format of the CA certificate. Default value: PEM Possible values = DER, PEM
cakey	<String>	Read-write	Private key, associated with the CA certificate that is used to sign the Intermediate-CA certificate or the end-user client and server certificate. If the CA key file is password protected, the user is prompted to enter the pass phrase that was used to encrypt the key.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum length = 63
cakeyform	<String>	Read-write	Format for the CA certificate. Default value: PEM Possible values = DER, PEM
caserial	<String>	Read-write	Serial number file maintained for the CA certificate. This file contains the serial number of the next certificate to be issued or signed by the CA. If the specified file does not exist, a new file is created, with /nsconfig/ssl/ as the default path. If you do not specify a proper path for the existing serial file, a new serial file is created. This might change the certificate serial numbers assigned by the CA certificate to each of the certificates it signs. Maximum length = 63

Operations

(click to see Properties)

- CREATE

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

CREATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcert? **action=create HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"sslcert":{

<b>"certfile":<String_value>,
```

```
</b><b>"reqfile":<String_value>,

</b><b>"certtype":<String_value>,

</b>"keyfile":<String_value>,

"keyform":<String_value>,

"pempassphrase":<String_value>,

"days":<Integer_value>,

"subjectaltname":<String_value>,

"certform":<String_value>,

"cacert":<String_value>,

"cacertform":<String_value>,

"cakey":<String_value>,

"cakeyform":<String_value>,

"caserial":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

sslcertbundle

Configuration for Imported Certbundle resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name to assign to the imported certificate bundle. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my file" or 'my file'). Minimum length = 1 Maximum length = 31
src	<String>	Read-write	URL specifying the protocol, host, and path, including file name, to the certificate bundle to be imported or exported. For example, http://

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			www.example.com/cert_bundle_file. NOTE: The import fails if the object to be imported is on an HTTPS server that requires client certificate authentication for access, and the issuer certificate of the HTTPS server is not present in the specific path on NetScaler to authenticate the HTTPS server. Minimum length = 1 Maximum length = 2047
inuse	<String>	Read-only	. Possible values = YES, NO
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- IMPORT
- DELETE
- GET (ALL)

- COUNT
- APPLY
- EXPORT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

IMPORT

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcertbundle? **action=Import HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"sslcertbundle":{

<b>"name":<String_value>,

</b><b>"src":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcertbundle **Query-parameters: args= name:<String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

APPLY

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcertbundle? **action=apply HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"sslcertbundle":{

<b>"name":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

EXPORT

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcertbundle? **action=export HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"sslcertbundle":{

<b>"name":<String_value>,

</b><b>"src":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcertbundle **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/sslcertbundle? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/sslcertbundle? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of sslcertbundle resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/sslcertbundle? **view=summary**

Use this query-parameter to get the summary output of sslcertbundle resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/sslcertbundle? **pagesize=#no;pageno=#no**

Use this query-parameter to get the sslcertbundle resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "sslcertbundle": [ {

"name":<String_value>,

"inuse":<String_value>,
```

```
"src":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcertbundle? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "sslcertbundle": [ { "__count": "#no"} ] }
```

sslcertchain

Configuration for CERT Chain resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
certkeyname	<String>	Read-write	Name of the Certificate. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcertchain **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/sslcertchain? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/sslcertchain? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of sslcertchain resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/sslcertchain? **view=summary**

Use this query-parameter to get the summary output of sslcertchain resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/sslcertchain? **pagesize=#no;pageno=#no**

Use this query-parameter to get the sslcertchain resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "sslcertchain": [ {

"certkeyname":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcertchain/ certkeyname_value<String>
Query-parameters: attrs http:// <netscaler-ip-address> /nitro/v1/config/sslcertchain/ certkeyname_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/sslcertchain/ certkeyname_value<String> ? **view=summary**

Use this query-parameter to get the summary output of sslcertchain resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslcertchain": [ {

"certkeyname":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcertchain? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "sslcertchain": [ { "__count": "#no"} ] }
```

sslcertchain_binding

Binding object which returns the resources bound to sslcertchain.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
certkeyname	<String>	Read-write	Name of the Certificate. Minimum length = 1
sslcertchain_sslcertkey_binding	<sslcertchain_sslcertkey_binding[]>	Read-only	sslcertkey that can be bound to sslcertchain.

Operations

(click to see Properties)

- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcertchain_binding/ certkeyname_value<String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "sslcertchain_binding": [ {

"certkeyname":<String_value>,

"sslcertchain_sslcertkey_binding":<sslcertchain_sslcertkey_binding[]_value
>

}]}
```

sslcertchain_sslcertkey_binding

Binding object showing the sslcertkey that can be bound to sslcertchain.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
linkcertkeyname	<String>	Read-write	Name of the Linked Certificate. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
certkeyname	<String>	Read-write	Name of the Certificate. Minimum length = 1
addsubject	<Boolean>	Read-only	Used to find if certificate is linked.
islinked	<Boolean>	Read-only	Used to find if certificate is linked.
isca	<Boolean>	Read-only	Used to find if certificate is a CA.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcertchain_sslcertkey_binding/ certkeyname_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/ config/sslcertchain_sslcertkey_binding/ certkeyname_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of sslcertchain_sslcertkey_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/sslcertchain_sslcertkey_binding/ certkeyname_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the sslcertchain_sslcertkey_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslcertchain_sslcertkey_binding": [ {

"linkcertkeyname":<String_value>,
```

```
"certkeyname":<String_value>,

"addsubject":<Boolean_value>,

"islinked":<Boolean_value>,

"isca":<Boolean_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcertchain_sslcertkey_binding/ certkeyname_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"sslcertchain_sslcertkey_binding": [ { "__count": "#no"} ] }
```

sslcertfile

Configuration for Imported Certfile resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name to assign to the imported certificate file. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my file" or 'my file'). Minimum length = 1 Maximum length = 31
src	<String>	Read-write	URL specifying the protocol, host, and path, including file name, to the certificate file to be imported. For example, http://www.example.com/cert_file.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			NOTE: The import fails if the object to be imported is on an HTTPS server that requires client certificate authentication for access, and the issuer certificate of the HTTPS server is not present in the specific path on NetScaler to authenticate the HTTPS server. Minimum length = 1 Maximum length = 2047
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- IMPORT
- DELETE
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

IMPORT

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcertfile? **action=Import HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"sslcertfile":{

<b>"name":<String_value>,

</b><b>"src":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcertfile **Query-parameters: args= name:<String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcertfile **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/sslcertfile? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/sslcertfile? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of sslcertfile resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/sslcertfile? **view=summary**

Use this query-parameter to get the summary output of sslcertfile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/sslcertfile? **pagesize=#no;pageno=#no**

Use this query-parameter to get the sslcertfile resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "sslcertfile": [ {

"name":<String_value>,

"src":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcertfile? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "sslcertfile": [ { "__count": "#no"} ] }
```

sslcertificatechain

Configuration for linked certificate resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
certkeyname	<String>	Read-write	Name of the certificate-key pair.
chainlinked	<String[]>	Read-only	Certkeys which are currenlty in SSL certificate chain.
chainpossiblelinks	<String[]>	Read-only	Certkeys which can be in SSL certificate chain.
chainissuer	<String>	Read-only	Name of the issuer.
chaincomplete	<Integer>	Read-only	Is set to 1 if ssl certificate chain is complete.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- GET (ALL)

- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcertificatechain

HTTP Method: POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"sslcertificatechain":{

<b>"certkeyname":<String_value>

</b>}}
```

Response:

HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcertificatechain

Query-parameters:

attrs

http:// <netscaler-ip-address> /nitro/v1/config/sslcertificatechain? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter

http:// <netscaler-ip-address> /nitro/v1/config/sslcertificatechain? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of sslcertificatechain resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view

http:// <netscaler-ip-address> /nitro/v1/config/sslcertificatechain? **view=summary**

Use this query-parameter to get the summary output of sslcertificatechain resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination

http:// <netscaler-ip-address> /nitro/v1/config/sslcertificatechain? **pagesize=#no;pageno=#no**

Use this query-parameter to get the sslcertificatechain resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "sslcertificatechain": [ {

"certkeyname":<String_value>,

"chainlinked":<String[]_value>,

"chainpossiblelinks":<String[]_value>,

"chainissuer":<String_value>,

"chaincomplete":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcertificatechain/ certkeyname_value<String>

Query-parameters:

attrs

http:// <netscaler-ip-address> /nitro/v1/config/sslcertificatechain/ certkeyname_value<String> ?**attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view

http:// <netscaler-ip-address> /nitro/v1/config/sslcertificatechain/ certkeyname_value<String> ?**view=summary**

Use this query-parameter to get the summary output of sslcertificatechain resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslcertificatechain": [ {

"certkeyname":<String_value>,

"chainlinked":<String[]_value>,

"chainpossiblelinks":<String[]_value>,

"chainissuer":<String_value>,

"chaincomplete":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcertificatechain? **count=yes**

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "sslcertificatechain": [ { "__count": "#no"} ] }
```

sslcertkey

Configuration for certificate key resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
certkey	<String>	Read-write	Name for the certificate and private-key pair. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the certificate-key pair is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			single quotation marks (for example, "my cert" or 'my cert'). Minimum length = 1
cert	<String>	Read-write	Name of and, optionally, path to the X509 certificate file that is used to form the certificate-key pair. The certificate file should be present on the appliance's hard-disk drive or solid-state drive. Storing a certificate in any location other than the default might cause inconsistency in a high availability setup. /nsconfig/ssl/ is the default path. Minimum length = 1
key	<String>	Read-write	Name of and, optionally, path to the private-key file that is used to form the certificate-key pair. The certificate file should be present on the appliance's hard-disk drive or solid-state drive. Storing a certificate in any location other than the default might cause inconsistency

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			in a high availability setup. /nsconfig/ssl/ is the default path. Minimum length = 1
password	<Boolean>	Read-write	Passphrase that was used to encrypt the private-key. Use this option to load encrypted private-keys in PEM format.
fipskey	<String>	Read-write	Name of the FIPS key that was created inside the Hardware Security Module (HSM) of a FIPS appliance, or a key that was imported into the HSM. Minimum length = 1
hsmkey	<String>	Read-write	Name of the HSM key that was created in the External Hardware Security Module (HSM) of a FIPS appliance. Minimum length = 1
inform	<String>	Read-write	Input format of the certificate and the private-key files. The three formats supported by the appliance are: PEM - Privacy Enhanced Mail

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			DER - Distinguished Encoding Rule PFX - Personal Information Exchange. Default value: PEM Possible values = DER, PEM, PFX
passplain	<String>	Read-write	Pass phrase used to encrypt the private-key. Required when adding an encrypted private-key in PEM format. Minimum length = 1
expirymonitor	<String>	Read-write	Issue an alert when the certificate is about to expire. Possible values = ENABLED, DISABLED
notificationperiod	<Integer>	Read-write	Time, in number of days, before certificate expiration, at which to generate an alert that the certificate is about to expire. Minimum value = 10 Maximum value = 100

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
bundle	<String>	Read-write	Parse the certificate chain as a single file after linking the server certificate to its issuer's certificate within the file. Default value: NO Possible values = YES, NO
deletecertkeyfilesonremoval	<String>	Read-write	This option is used to automatically delete certificate/key files from physical device when the added certkey is removed. When deleteCertKeyFilesOnRemoval option is used at rm certkey command, it overwrites the deleteCertKeyFilesOnRemoval setting used at add/set certkey command. Default value: CERTKEYFILE_DELETE_NO Possible values = NO, ALWAYS, IF_EXPIRED
deletefromdevice	<Boolean>	Read-write	Delete cert/key file from file system.
linkcertkeyname	<String>	Read-write	Name of the Certificate Authority

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			certificate-key pair to which to link a certificate-key pair. Minimum length = 1
nodomaincheck	<Boolean>	Read-write	Override the check for matching domain names during a certificate update operation.
ocspstaplingcache	<Boolean>	Read-write	Clear cached ocspStapling response in certkey.
signaturealg	<String>	Read-only	Signature algorithm.
certificatetype	<String[]>	Read-only	Specifies whether the certificate is of type root-CA, intermediate-CA, server, client, or client and server. Possible values = ROOT_CERT, INTM_CERT, CLNT_CERT, SRVR_CERT, UNKNOWN_CERT
serial	<String>	Read-only	Serial number.
issuer	<String>	Read-only	Issuer name.
clientcertnotbefore	<String>	Read-only	Not-Before date.
clientcertnotafter	<String>	Read-only	Not-After date.
daystoexpiration	<Integer>	Read-only	Days remaining for the certificate to expire.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
subject	<String>	Read-only	Subject name.
publickey	<String>	Read-only	Public key algorithm.
publickeysize	<Integer>	Read-only	Size of the public key.
version	<Integer>	Read-only	Version.
priority	<Integer>	Read-only	ocsp priority.
status	<String>	Read-only	Status of the certificate. Possible values = Valid, Not yet valid, Expired
passcrypt	<String>	Read-only	Passcrypt. Minimum length = 1
data	<Integer>	Read-only	Vserver Id.
servicename	<String>	Read-only	Service name to which the certificate key pair is bound.
sandns	<String>	Read-only	Subject Alternative Name (SAN) is an extension to X.509 that allows various values to be associated with a security certificate using a subjectAltName field. These values are called "Subject Alternative Names" (SAN). This field is for DNS names.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
sanipadd	<String>	Read-only	Subject Alternative Name (SAN) is an extension to X.509 that allows various values to be associated with a security certificate using a subjectAltName field. These values are called "Subject Alternative Names" (SAN). This field is for IP address.
ocspresponsestatus	<String>	Read-only	Ocsp response status of the certificate. Possible values = NONE, EXPIRED, VALID
builtin	<String[]>	Read-only	Flag to determine if Cert key is built-in or not. Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL
feature	<String>	Read-only	The feature to be checked while applying this config.
certkeydigest	<String>	Read-only	Stores the added md5sum of

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			certificate and key files.
certificatesource	<String>	Read-only	Location of the certificate. Default value: LOCAL Possible values = LOCAL, REMOTE
certkeystatus	<String>	Read-only	Status of the certkey in PE. Possible values = ACTIVE, INACTIVE(Default state), INACTIVE(No Private Key), INACTIVE(Duplicate SAN-Multiple clashing certs), INACTIVE(Duplicate SAN-All SAN entires not covered), INACTIVE(Duplicate SAN-Earlier expiry), INACTIVE(Crossed MAX SAN limit), INACTIVE(No common name), INACTIVE(Common name/SAN too long), INACTIVE(No memory),

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			INACTIVE(MAX cert req len reached), INACTIVE(X509 Name failure)
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- LINK
- UNLINK
- GET (ALL)
- GET
- COUNT
- CHANGE
- CLEAR

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcertkey **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"sslcertkey":{

<b>"certkey":<String_value>,

</b><b>"cert":<String_value>,

</b>"key":<String_value>,

"password":<Boolean_value>,

"fipskey":<String_value>,

"hsmkey":<String_value>,

"inform":<String_value>,
```

```
"passplain":<String_value>,

"expirymonitor":<String_value>,

"notificationperiod":<Integer_value>,

"bundle":<String_value>,

"deletecertkeyfilesonremoval":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcertkey/ certkey_value<String> **Query-parameters: args=deletefromdevice: <Boolean_value> ,deletecertkeyfilesonremoval: <String_value>**
update
URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcertkey **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"sslcertkey":{

<b>"certkey":<String_value>,

</b>"expirymonitor":<String_value>,

"notificationperiod":<Integer_value>,

"deletecertkeyfilesonremoval":<String_value>
```

```
}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

unset

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcertkey? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"sslcertkey":{

<b>"certkey":<String_value>,

</b>"expirymonitor":true,

"notificationperiod":true,

"deletecertkeyfilesonremoval":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

link

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcertkey? **action=link HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"sslcertkey":{

<b>"certkey":<String_value>,

</b><b>"linkcertkeyname":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

unlink

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcertkey? **action=unlink HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"sslcertkey":{

<b>"certkey":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

change

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcertkey? **action=update HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"sslcertkey":{

<b>"certkey":<String_value>,

</b>"cert":<String_value>,

"key":<String_value>,

"password":<Boolean_value>,

"fipskey":<String_value>,

"inform":<String_value>,

"passplain":<String_value>,

"nodomaincheck":<Boolean_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

clear

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcertkey? **action=clear HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"sslcertkey":{

<b>"certkey":<String_value>,

</b>"ocspstaplingcache":<Boolean_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error
get (all)
URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcertkey **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/sslcertkey? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/sslcertkey? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of sslcertkey resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/sslcertkey? **view=summary**

Use this query-parameter to get the summary output of sslcertkey resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/sslcertkey? **pagesize=#no;pageno=#no**

Use this query-parameter to get the sslcertkey resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "sslcertkey": [ {

"certkey":<String_value>,

"cert":<String_value>,

"key":<String_value>,

"inform":<String_value>,

"signaturealg":<String_value>,

"certificatetype":<String[]_value>,

"serial":<String_value>,

"issuer":<String_value>,

"clientcertnotbefore":<String_value>,

"clientcertnotafter":<String_value>,

"daystoexpiration":<Integer_value>,

"subject":<String_value>,

"publickey":<String_value>,

"publickeysize":<Integer_value>,
```

```
"version":<Integer_value>,

"priority":<Integer_value>,

"status":<String_value>,

"fipskey":<String_value>,

"hsmkey":<String_value>,

"passcrypt":<String_value>,

"passplain":<String_value>,

"data":<Integer_value>,

"servicename":<String_value>,

"expirymonitor":<String_value>,

"notificationperiod":<Integer_value>,

"linkcertkeyname":<String_value>,

"sandns":<String_value>,

"sanipadd":<String_value>,

"ocspresponsestatus":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"certkeydigest":<String_value>,

"certificatesource":<String_value>,

"certkeystatus":<String_value>,

"deletecertkeyfilesonremoval":<String_value>,

"_nextgenapiresource":<String_value>
```

```
}]}
```

get
URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcertkey/ certkey_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/sslcertkey/ certkey_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/sslcertkey/ certkey_value<String> ? **view=summary**

Use this query-parameter to get the summary output of sslcertkey resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslcertkey": [ {

"certkey":<String_value>,

"cert":<String_value>,
```

```
"key":<String_value>,

"inform":<String_value>,

"signaturealg":<String_value>,

"certificatetype":<String[]_value>,

"serial":<String_value>,

"issuer":<String_value>,

"clientcertnotbefore":<String_value>,

"clientcertnotafter":<String_value>,

"daystoexpiration":<Integer_value>,

"subject":<String_value>,

"publickey":<String_value>,

"publickeysize":<Integer_value>,

"version":<Integer_value>,

"priority":<Integer_value>,

"status":<String_value>,

"fipskey":<String_value>,

"hsmkey":<String_value>,

"passcrypt":<String_value>,

"passplain":<String_value>,

"data":<Integer_value>,

"servicename":<String_value>,

"expirymonitor":<String_value>,
```

```
"notificationperiod":<Integer_value>,

"linkcertkeyname":<String_value>,

"sandns":<String_value>,

"sanipadd":<String_value>,

"ocspresponsestatus":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"certkeydigest":<String_value>,

"certificatesource":<String_value>,

"certkeystatus":<String_value>,

"deletecertkeyfilesonremoval":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

count

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcertkey? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "sslcertkey": [ { "__count": "#no"} ] }
```

sslcertkey_binding

Binding object which returns the resources bound to sslcertkey.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
certkey	<String>	Read-write	Name of the certificate-key pair for which to show detailed information. Minimum length = 1
sslcertkey_sslvserver_binding	<sslcertkey_sslvserver_binding[]>	Read-only	sslvserver that can be bound to sslcertkey.
sslcertkey_crldistribution_binding	<sslcertkey_crldistribution_binding[]>	Read-only	crldistribution that can be bound to sslcertkey.
sslcertkey_sslprofile_binding	<sslcertkey_sslprofile_binding[]>	Read-only	sslprofile that can be bound to sslcertkey.
sslcertkey_service_binding	<sslcertkey_service_binding[]>	Read-only	service that can be bound to sslcertkey.
sslcertkey_sslocspresponder_binding	<sslcertkey_sslocspresponder_binding[]>	Read-only	sslocspresponder that can be bound to sslcertkey.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcertkey_binding/ certkey_value<String>
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "sslcertkey_binding": [ {

"certkey":<String_value>,

"sslcertkey_sslvserver_binding":<sslcertkey_sslvserver_binding[]_value>,

"sslcertkey_crldistribution_binding":<sslcertkey_crldistribution_binding[]
_value>,

"sslcertkey_sslprofile_binding":<sslcertkey_sslprofile_binding[]_value>,

"sslcertkey_service_binding":<sslcertkey_service_binding[]_value>,

"sslcertkey_sslocspresponder_binding":<sslcertkey_sslocspresponder_binding
[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcertkey_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/sslcertkey_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "sslcertkey_binding": [ {

"certkey":<String_value>,

"sslcertkey_sslvserver_binding":<sslcertkey_sslvserver_binding[]_value>,

"sslcertkey_crldistribution_binding":<sslcertkey_crldistribution_binding[]
_value>,

"sslcertkey_sslprofile_binding":<sslcertkey_sslprofile_binding[]_value>,

"sslcertkey_service_binding":<sslcertkey_service_binding[]_value>,

"sslcertkey_sslocspresponder_binding":<sslcertkey_sslocspresponder_binding
[]_value>

}]}
```

sslcertkey_crldistribution_binding

Binding object showing the crldistribution that can be bound to sslcertkey.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
certkey	<String>	Read-write	Name of the certificate-key pair. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ca	<Boolean>	Read-write	The certificate-key pair being unbound is a Certificate Authority (CA) certificate. If you choose this option, the certificate-key pair is unbound from the list of CA certificates that were bound to the specified SSL virtual server or SSL service.
issuer	<String>	Read-write	Issuer name.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of

creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcertkey_crldistribution_binding/ certkey_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ sslcertkey_crldistribution_binding/ certkey_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of sslcertkey_crldistribution_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/sslcertkey_crldistribution_binding/ certkey_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the sslcertkey_crldistribution_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslcertkey_crldistribution_binding": [ {

"certkey":<String_value>,

"ca":<Boolean_value>,

"issuer":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcertkey_crldistribution_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/sslcertkey_crldistribution_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslcertkey_crldistribution_binding": [ {

"certkey":<String_value>,

"ca":<Boolean_value>,

"issuer":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcertkey_crldistribution_binding/ certkey_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"sslcertkey_crldistribution_binding": [ { "__count": "#no"} ] }
```

sslcertkey_service_binding

Binding object showing the service that can be bound to sslcertkey.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
certkey	<String>	Read-write	Name of the certificate-key pair. Minimum length = 1
service	<Boolean>	Read-write	Bind the certificate to the named SSL service or service group.
servicename	<String>	Read-write	Service name to which the certificate key pair is bound.
ca	<Boolean>	Read-write	The certificate-key pair being unbound is a Certificate Authority (CA) certificate. If you choose this option, the certificate-key pair is unbound from the list of CA certificates that were bound to the specified SSL virtual server or SSL service.
servicegroupname	<String>	Read-write	The name of the SSL service group to which the certificate-key pair needs to be bound. Use the "add servicegroup" command to create this service. Minimum length = 1
version	<Integer>	Read-only	Version.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
data	<Integer>	Read-only	Vserver Id.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcertkey_service_binding/ certkey_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ sslcertkey_service_binding/ certkey_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of sslcertkey_service_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/sslcertkey_service_binding/ certkey_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the sslcertkey_service_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslcertkey_service_binding": [ {

"certkey":<String_value>,

"service":<Boolean_value>,

"servicename":<String_value>,

"ca":<Boolean_value>,

"servicegroupname":<String_value>,
```

```
"version":<Integer_value>,

"data":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcertkey_service_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/sslcertkey_service_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslcertkey_service_binding": [ {

"certkey":<String_value>,

"service":<Boolean_value>,

"servicename":<String_value>,
```

```
"ca":<Boolean_value>,

"servicegroupname":<String_value>,

"version":<Integer_value>,

"data":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcertkey_service_binding/ certkey_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"sslcertkey_service_binding": [ { "__count": "#no"} ] }
```

sslcertkey_sslocspresponder_binding

Binding object showing the sslocspresponder that can be bound to sslcertkey.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
priority	<Integer>	Read-write	ocsp priority.
ocspresponder	<String>	Read-write	OCSP responders bound to this certkey.
certkey	<String>	Read-write	Name of the certificate-key pair. Minimum length = 1
ca	<Boolean>	Read-write	The certificate-key pair being unbound is a Certificate Authority (CA) certificate. If you choose this option, the certificate-key pair is unbound from the list of CA certificates that were bound to the specified SSL virtual server or SSL service.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/sslcertkey_sslocspresponder_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"sslcertkey_sslocspresponder_binding":{

"certkey":<String_value>,
```

```
"ocspresponder":<String_value>,

"priority":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcertkey_sslocspresponder_binding/ certkey_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ sslcertkey_sslocspresponder_binding/ certkey_value<String> ? **args=ocspresponder: <String_value> ,ca: <Boolean_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcertkey_sslocspresponder_binding/ certkey_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ sslcertkey_sslocspresponder_binding/ certkey_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of sslcertkey_sslocspresponder_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/sslcertkey_sslocspresponder_binding/ certkey_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the sslcertkey_sslocspresponder_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslcertkey_sslocspresponder_binding": [ {

"priority":<Integer_value>,

"ocspresponder":<String_value>,

"certkey":<String_value>,

"ca":<Boolean_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcertkey_sslocspresponder_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/sslcertkey_sslocspresponder_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslcertkey_sslocspresponder_binding": [ {

"priority":<Integer_value>,

"ocspresponder":<String_value>,

"certkey":<String_value>,

"ca":<Boolean_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcertkey_sslocspresponder_binding/ certkey_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"sslcertkey_sslocspresponder_binding": [ { "__count": "#no"} ] }
```

sslcertkey_sslprofile_binding

Binding object showing the sslprofile that can be bound to sslcertkey.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
sslprofile	<String>	Read-write	SSL profile name to which the certificate key pair is bound.
certkey	<String>	Read-write	Name of the certificate-key pair. Minimum length = 1
ca	<Boolean>	Read-write	The certificate-key pair being unbound is a Certificate Authority (CA) certificate. If you choose this option, the certificate-key pair is unbound from the list of CA certificates that were bound to the specified SSL virtual server or SSL service.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcertkey_sslprofile_binding/ certkey_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ sslcertkey_sslprofile_binding/ certkey_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of sslcertkey_sslprofile_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/sslcertkey_sslprofile_binding/ certkey_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the sslcertkey_sslprofile_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslcertkey_sslprofile_binding": [ {

"sslprofile":<String_value>,

"certkey":<String_value>,

"ca":<Boolean_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcertkey_sslprofile_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/sslcertkey_sslprofile_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslcertkey_sslprofile_binding": [ {

"sslprofile":<String_value>,

"certkey":<String_value>,

"ca":<Boolean_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcertkey_sslprofile_binding/certkey_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"sslcertkey_sslprofile_binding": [ { "__count": "#no"} ] }
```

sslcertkey_sslvserver_binding

Binding object showing the sslvserver that can be bound to sslcertkey.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
servername	<String>	Read-write	Vserver name to which the certificate key pair is bound.
vserver	<Boolean>	Read-write	Specify this option to bind the certificate to an SSL virtual server. Note: The default option is -vServer.
certkey	<String>	Read-write	Name of the certificate-key pair. Minimum length = 1
vservername	<String>	Read-write	The name of the SSL virtual server name to which the certificate-key pair needs to be bound. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ca	<Boolean>	Read-write	The certificate-key pair being unbound is a Certificate Authority (CA) certificate. If you choose this option, the certificate-key pair is unbound from the list of CA certificates that were bound to the specified SSL virtual server or SSL service.
data	<Integer>	Read-only	Vserver Id.
version	<Integer>	Read-only	Version.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcertkey_sslvserver_binding/ certkey_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ sslcertkey_sslvserver_binding/ certkey_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of sslcertkey_sslvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/sslcertkey_sslvserver_binding/ certkey_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the sslcertkey_sslvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslcertkey_sslvserver_binding": [ {

"servername":<String_value>,

"vserver":<Boolean_value>,

"certkey":<String_value>,

"vservername":<String_value>,

"ca":<Boolean_value>,

"data":<Integer_value>,

"version":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcertkey_sslvserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/sslcertkey_sslvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslcertkey_sslvserver_binding": [ {

"servername":<String_value>,

"vserver":<Boolean_value>,

"certkey":<String_value>,

"vservername":<String_value>,

"ca":<Boolean_value>,

"data":<Integer_value>,

"version":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcertkey_sslvserver_binding/ certkey_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"sslcertkey_sslvserver_binding": [ { "__count": "#no"} ] }
```

sslcertkeybundle

Configuration for certkey bundle resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
certkeybundlename	<String>	Read-write	Name given to the cerKeyBundle. The name will be used to bind/unbind certkey bundle to vip. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			quotation marks (for example, "my file" or 'my file'). Minimum length = 1 Maximum length = 127
bundlefile	<String>	Read-write	Name of and, optionally, path to the X509 certificate bundle file that is used to form the certificate-key bundle. The certificate bundle file should be present on the appliance's hard-disk drive or solid-state drive. /nsconfig/ssl/ is the default path. The certificate bundle file consists of list of certificates and one key in PEM format. Minimum length = 1
passplain	<String>	Read-write	Pass phrase used to encrypt the private-key. Required when certificate bundle file contains encrypted private-key in PEM format.
certkeybundledigest	<String>	Read-only	Stores the digest of certificate and key bundle file.
_nextgenapiresource	<String>	Read-only	.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- CHANGE
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcertkeybundle **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"sslcertkeybundle":{

<b>"certkeybundlename":<String_value>,

</b><b>"bundlefile":<String_value>,

</b>"passplain":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcertkeybundle/ certkeybundlename_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

CHANGE

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcertkeybundle? **action=update HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"sslcertkeybundle":{

<b>"certkeybundlename":<String_value>,

</b>"bundlefile":<String_value>,

"passplain":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcertkeybundle **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/sslcertkeybundle? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/sslcertkeybundle? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of sslcertkeybundle resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/sslcertkeybundle? **view=summary**

Use this query-parameter to get the summary output of sslcertkeybundle resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/sslcertkeybundle? **pagesize=#no;pageno=#no**

Use this query-parameter to get the sslcertkeybundle resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "sslcertkeybundle": [ {

"certkeybundlename":<String_value>,

"bundlefile":<String_value>,

"passplain":<String_value>,

"certkeybundledigest":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcertkeybundle/ certkeybundlename_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/sslcertkeybundle/ certkeybundlename_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/sslcertkeybundle/ certkeybundlename_value<String> ? **view=summary**

Use this query-parameter to get the summary output of sslcertkeybundle resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslcertkeybundle": [ {

"certkeybundlename":<String_value>,

"bundlefile":<String_value>,

"passplain":<String_value>,

"certkeybundledigest":<String_value>,
```

```
"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcertkeybundle? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "sslcertkeybundle": [ { "__count": "#no"} ] }
```

sslcertkeybundle_binding

Binding object which returns the resources bound to sslcertkeybundle.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
certkeybundlename	<String>	Read-write	Name given to the cerKeyBundle. The name will be used to bind/unbind certkey

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			bundle to vip. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my file" or 'my file'). Minimum length = 1 Maximum length = 127
sslcertkeybundle_sslvserver_binding	<sslcertkeybundle_sslvserver_binding[]>	Read-only	sslvserver that can be bound to sslcertkeybundle.
sslcertkeybundle_intermediatecertlinks_binding	<sslcertkeybundle_intermediatecertlinks_binding[]>	Read-only	intermediatecertlinks that can be bound to sslcertkeybundle.

Operations

(click to see Properties)

- GET

- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcertkeybundle_binding/ certkeybundlename_value<String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "sslcertkeybundle_binding": [ {

"certkeybundlename":<String_value>,

"sslcertkeybundle_intermediatecertlinks_binding":<sslcertkeybundle_interme
diatecertlinks_binding[]_value>,

"sslcertkeybundle_sslvserver_binding":<sslcertkeybundle_sslvserver_binding
[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcertkeybundle_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/sslcertkeybundle_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "sslcertkeybundle_binding": [ {

"certkeybundlename":<String_value>,

"sslcertkeybundle_intermediatecertlinks_binding":<sslcertkeybundle_interme
diatecertlinks_binding[]_value>,

"sslcertkeybundle_sslvserver_binding":<sslcertkeybundle_sslvserver_binding
[]_value>

}]}
```

sslcertkeybundle_intermediatecertlinks_binding

Binding object showing the intermediatecertlinks that can be bound to sslcertkeybundle.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
certkeybundlename	<String>	Read-write	Name given to the cerKeyBundle. The name will be used to bind/unbind certkey bundle to vip. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. The following

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my file" or 'my file'). Minimum length = 1 Maximum length = 127
subject	<String>	Read-write	Subject name.
daystoexpiration	<Integer>	Read-only	Days remaining for the certificate to expire.
sandns	<String>	Read-only	Subject Alternative Name (SAN) is an extension to X.509 that allows various values to be associated with a security certificate using a subjectAltName field. These values are called "Subject Alternative Names" (SAN). This field is for DNS names.
issuer	<String>	Read-only	Issuer name.
clientcertnotbefore	<String>	Read-only	Not-Before date.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
status	<String>	Read-only	Status of the certificate. Possible values = Valid, Not yet valid, Expired
clientcertnotafter	<String>	Read-only	Not-After date.
publickey	<String>	Read-only	Public key algorithm.
sanipadd	<String>	Read-only	Subject Alternative Name (SAN) is an extension to X.509 that allows various values to be associated with a security certificate using a subjectAltName field. These values are called "Subject Alternative Names" (SAN). This field is for IP address.
signaturealg	<String>	Read-only	Signature algorithm.
serial	<String>	Read-only	Serial number.
publickeysize	<Integer>	Read-only	Size of the public key.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)

- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcertkeybundle_intermediatecertlinks_binding/ certkeybundlename_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/sslcertkeybundle_intermediatecertlinks_binding/ certkeybundlename_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of sslcertkeybundle_intermediatecertlinks_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/sslcertkeybundle_intermediatecertlinks_binding/ certkeybundlename_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the sslcertkeybundle_intermediatecertlinks_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslcertkeybundle_intermediatecertlinks_binding": [ {

"certkeybundlename":<String_value>,

"subject":<String_value>,

"daystoexpiration":<Integer_value>,

"sandns":<String_value>,

"issuer":<String_value>,

"clientcertnotbefore":<String_value>,

"status":<String_value>,

"clientcertnotafter":<String_value>,

"publickey":<String_value>,

"sanipadd":<String_value>,
```

```
"signaturealg":<String_value>,

"serial":<String_value>,

"publickeysize":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcertkeybundle_intermediatecertlinks_binding
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/sslcertkeybundle_intermediatecertlinks_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslcertkeybundle_intermediatecertlinks_binding": [ {

"certkeybundlename":<String_value>,

"subject":<String_value>,
```

```
"daystoexpiration":<Integer_value>,

"sandns":<String_value>,

"issuer":<String_value>,

"clientcertnotbefore":<String_value>,

"status":<String_value>,

"clientcertnotafter":<String_value>,

"publickey":<String_value>,

"sanipadd":<String_value>,

"signaturealg":<String_value>,

"serial":<String_value>,

"publickeysize":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/ sslcertkeybundle_intermediatecertlinks_binding/ certkeybundlename_value<String> ? **count=yes**
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"sslcertkeybundle_intermediatecertlinks_binding": [ { "__count":
"#no"} ] }
```

sslcertkeybundle_sslvserver_binding

Binding object showing the sslvserver that can be bound to sslcertkeybundle.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
servername	<String>	Read-write	Vserver name to which the certKeyBundle is bound.
certkeybundlename	<String>	Read-write	Name given to the cerKeyBundle. The name will be used to bind/unbind certkey bundle to vip. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. The following requirement applies only to the Citrix ADC CLI: If the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my file" or 'my file'). Minimum length = 1 Maximum length = 127
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcertkeybundle_sslvserver_binding/ certkeybundlename_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/sslcertkeybundle_sslvserver_binding/ certkeybundlename_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of sslcertkeybundle_sslvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/sslcertkeybundle_sslvserver_binding/ certkeybundlename_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the sslcertkeybundle_sslvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslcertkeybundle_sslvserver_binding": [ {

"servername":<String_value>,

"certkeybundlename":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcertkeybundle_sslvserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/sslcertkeybundle_sslvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslcertkeybundle_sslvserver_binding": [ {

"servername":<String_value>,

"certkeybundlename":<String_value>
```

```
}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcertkeybundle_sslvserver_binding/ certkeybundlename_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"sslcertkeybundle_sslvserver_binding": [ { "__count": "#no"} ] }
```

sslcertlink

Configuration for linked certificate resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
certkeyname	<String>	Read-write	Certificate key name.
linkcertkeyname	<String>	Read-write	Name of the Certificate-Authority.
_nextgenapiresource	<String>	Read-write	.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.
- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcertlink

Query-parameters:

attrs

http:// <netscaler-ip-address> /nitro/v1/config/sslcertlink? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter

http:// <netscaler-ip-address> /nitro/v1/config/sslcertlink? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of sslcertlink resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view

http:// <netscaler-ip-address> /nitro/v1/config/sslcertlink? **view=summary**

Use this query-parameter to get the summary output of sslcertlink resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination

http:// <netscaler-ip-address> /nitro/v1/config/sslcertlink? **pagesize=#no;pageno=#no**

Use this query-parameter to get the sslcertlink resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "sslcertlink": [ {

"certkeyname":<String_value>,

"linkcertkeyname":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcertlink? **count=yes**

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "sslcertlink": [ { "__count": "#no"} ] }
```

sslcertreq

Configuration for certificate request resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
reqfile	<String>	Read-write	Name for and, optionally, path to the certificate signing request (CSR). /nsconfig/ssl/ is the default path. Maximum length = 63
keyfile	<String>	Read-write	Name of and, optionally, path to the private key used to create the certificate signing request, which then becomes part of the certificate-key pair. The private key can be either an RSA or a DSA key. The key must be present in the appliance's local storage. /nsconfig/ssl is the default path. Maximum length = 63
subjectaltname	<String>	Read-write	Subject Alternative Name (SAN) is an extension to X.509 that allows various

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			values to be associated with a security certificate using a subjectAltName field. These values are called "Subject Alternative Names" (SAN). Names include: 1. Email addresses 2. IP addresses 3. URIs 4. DNS names (this is usually also provided as the Common Name RDN within the Subject field of the main certificate.) 5. Directory names (alternative Distinguished Names to that given in the Subject) Example:- subjectAltName "DNS:*.example.com DNS:www.example.org" . Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
fipskeyname	<String>	Read-write	Name of the FIPS key used to create the certificate signing request. FIPS keys are created inside the Hardware Security Module of the FIPS card. Minimum length = 1 Maximum length = 31
keyform	<String>	Read-write	Format in which the key is stored on the appliance. Default value: PEM Possible values = DER, PEM
pempassphrase	<String>	Read-write	. Minimum length = 1 Maximum length = 31
countryname	<String>	Read-write	Two letter ISO code for your country. For example, US for United States. Minimum length = 2 Maximum length = 2
statename	<String>	Read-write	Full name of the state or province where your

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			organization is located. Do not abbreviate. Minimum length = 1
organizationname	<String>	Read-write	Name of the organization that will use this certificate. The organization name (corporation, limited partnership, university, or government agency) must be registered with some authority at the national, state, or city level. Use the legal name under which the organization is registered. Do not abbreviate the organization name and do not use the following characters in the name: Angle brackets (< >) tilde (~), exclamation mark, at (@), pound (#), zero (0), caret (\^), asterisk (*), forward slash (/), square brackets ([ ]), question mark (?).

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum length = 1
organizationunitname	<String>	Read-write	Name of the division or section in the organization that will use the certificate. Minimum length = 1
localityname	<String>	Read-write	Name of the city or town in which your organization's head office is located. Minimum length = 1
commonname	<String>	Read-write	Fully qualified domain name for the company or web site. The common name must match the name used by DNS servers to do a DNS lookup of your server. Most browsers use this information for authenticating the server's certificate during the SSL handshake. If the server name in the URL does not match the common name as given in the server certificate, the browser terminates the SSL handshake or prompts the user with a warning message.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Do not use wildcard characters, such as asterisk (*) or question mark (?), and do not use an IP address as the common name. The common name must not contain the protocol specifier <http://> or <https://>. Minimum length = 1
emailaddress	<String>	Read-write	Contact person's e-mail address. This address is publically displayed as part of the certificate. Provide an e-mail address that is monitored by an administrator who can be contacted about the certificate. Minimum length = 1
challengepassword	<String>	Read-write	Pass phrase, embedded in the certificate signing request that is shared only between the client or server requesting the certificate and the SSL certificate issuer (typically the certificate authority). This pass phrase

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			can be used to authenticate a client or server that is requesting a certificate from the certificate authority. Minimum length = 4
companyname	<String>	Read-write	Additional name for the company or web site. Minimum length = 1
digestmethod	<String>	Read-write	Digest algorithm used in creating CSR. Possible values = SHA1, SHA256

Operations

(click to see Properties)

- CREATE

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.
- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

CREATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcertreq? **action=create HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"sslcertreq":{

<b>"reqfile":<String_value>,

</b>"keyfile":<String_value>,

"subjectaltname":<String_value>,

"fipskeyname":<String_value>,

"keyform":<String_value>,

"pempassphrase":<String_value>,

<b>"countryname":<String_value>,

</b><b>"statename":<String_value>,

</b><b>"organizationname":<String_value>,
```

```
</b>"organizationunitname":<String_value>,

"localityname":<String_value>,

"commonname":<String_value>,

"emailaddress":<String_value>,

"challengepassword":<String_value>,

"companyname":<String_value>,

"digestmethod":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

sslcipher

Configuration for cipher resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ciphergroupname	<String>	Read-write	Name for the user-defined cipher group. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@),

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			equals (=), and hyphen (-) characters. Cannot be changed after the cipher group is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my ciphergroup" or 'my ciphergroup'). Minimum length = 1
ciphgrpalias	<String>	Read-write	The individual cipher name(s), a user-defined cipher group, or a system predefined cipher alias that will be added to the predefined cipher alias that will be added to the group cipherGroupName. If a cipher alias or a cipher group is specified, all the individual ciphers in the cipher alias or group will be added

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			to the user-defined cipher group. Minimum length = 1
ciphername	<String>	Read-write	Cipher name.
cipherpriority	<Integer>	Read-write	This indicates priority assigned to the particular cipher. Minimum value = 1
sslprofile	<String>	Read-write	Name of the profile to which cipher is attached.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT
- DELETE

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcipher **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"sslcipher":{

<b>"ciphergroupname":<String_value>,

</b>"ciphgrpalias":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcipher **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"sslcipher":{

<b>"ciphergroupname":<String_value>,

</b>"ciphername":<String_value>,

"cipherpriority":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcipher? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"sslcipher":{

<b>"ciphergroupname":<String_value>,

</b>"ciphername":true,

"cipherpriority":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcipher/ ciphergroupname_value<String>
Query-parameters: args=ciphername: <String_value>
get (all)
URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcipher **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/sslcipher? **args=ciphergroupname: <String_value> ,sslprofile: <String_value>**

Use this query-parameter to get sslcipher resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/config/sslcipher? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/sslcipher? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of sslcipher resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/sslcipher? **view=summary**

Use this query-parameter to get the summary output of sslcipher resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/sslcipher? **pagesize=#no;pageno=#no**

Use this query-parameter to get the sslcipher resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "sslcipher": [ {

ciphergroupname:<String_value>,sslprofile:<String_value>"ciphername":<Stri
ng_value>,

"cipherpriority":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

get
URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcipher/ ciphergroupname_value<String>
Query-parameters: attrs http:// <netscaler-ip-address> /nitro/v1/config/sslcipher/ ciphergroupname_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/sslcipher/ ciphergroupname_value<String> ? **view=summary**

Use this query-parameter to get the summary output of sslcipher resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslcipher": [ {

ciphergroupname:<String_value>,sslprofile:<String_value>"ciphername":<Stri
ng_value>,

"cipherpriority":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

count

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcipher? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "sslcipher": [ { "__count": "#no"} ] }
```

sslcipher_binding

Binding object which returns the resources bound to sslcipher.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ciphergroupname	<String>	Read-write	Name of the cipher group for which to show detailed information. Minimum length = 1
sslcipher_sslciphersuite_binding	<sslcipher_sslciphersuite_binding[]>	Read-only	sslciphersuite that can be bound to sslcipher.
sslcipher_individualcipher_binding	<sslcipher_individualcipher_binding[]>	Read-only	individualcipher that can be bound to sslcipher.
sslcipher_sslprofile_binding	<sslcipher_sslprofile_binding[]>	Read-only	sslprofile that can be bound to sslcipher.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcipher_binding/ciphergroupname_value<String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "sslcipher_binding": [ {

"ciphergroupname":<String_value>,

"sslcipher_individualcipher_binding":<sslcipher_individualcipher_binding[]
_value>,

"sslcipher_sslciphersuite_binding":<sslcipher_sslciphersuite_binding[]_val
ue>,

"sslcipher_sslprofile_binding":<sslcipher_sslprofile_binding[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcipher_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/sslcipher_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "sslcipher_binding": [ {

"ciphergroupname":<String_value>,

"sslcipher_individualcipher_binding":<sslcipher_individualcipher_binding[]
_value>,

"sslcipher_sslciphersuite_binding":<sslcipher_sslciphersuite_binding[]_val
ue>,

"sslcipher_sslprofile_binding":<sslcipher_sslprofile_binding[]_value>

}]}
```

sslcipher_individualcipher_binding

Binding object showing the individualcipher that can be bound to sslcipher.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ciphgrpals	<String>	Read-write	A cipher-suite can consist of an individual cipher name, the system predefined cipher-alias name, or user defined cipher-group name. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
cipherpriority	<Integer>	Read-write	This indicates priority assigned to the particular cipher. Minimum value = 1
cipheroperation	<String>	Read-write	The operation that is performed when adding the cipher-suite.

Possible cipher operations are: ADD - Appends the given cipher-suite to the existing one configured for the virtual server. REM - Removes the given cipher-suite from the existing one configured for the virtual server. ORD - Overrides the current configured cipher-suite for the virtual server with the given cipher-suite.

Default value: 0

Possible values = ADD, REM, ORD

Minimum length = 1

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcipher_individualcipher_binding/ ciphergroupname_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/ config/sslcipher_individualcipher_binding/ ciphergroupname_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of sslcipher_individualcipher_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/sslcipher_individualcipher_binding/ ciphergroupname_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the sslcipher_individualcipher_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslcipher_individualcipher_binding": [ {

"ciphgrpals":<String_value>,

"cipherpriority":<Integer_value>,

"cipheroperation":<String_value>,

"ciphername":<String_value>,

"ciphergroupname":<String_value>,

"description":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcipher_individualcipher_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/sslcipher_individualcipher_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslcipher_individualcipher_binding": [ {

"ciphgrpals":<String_value>,

"cipherpriority":<Integer_value>,

"cipheroperation":<String_value>,

"ciphername":<String_value>,

"ciphergroupname":<String_value>,

"description":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcipher_individualcipher_binding/ciphergroupname_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"sslcipher_individualcipher_binding": [ { "__count": "#no"} ] }
```

sslcipher_service_binding

Binding object showing the service that can be bound to sslcipher.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
cipherpriority	<Integer>	Read-write	Priority of the cipher to be added. Minimum value = 1 Maximum value = 1000
cipheroperation	<String>	Read-write	The operation that is performed when adding the cipher-suite.

Possible cipher operations are: ADD - Appends the given cipher-suite to the existing one configured for the virtual server. REM - Removes the given cipher-suite from the existing one configured for the virtual server. ORD - Overrides the current configured cipher-suite for the virtual server with the given cipher-suite.

Default value: 0

Possible values = ADD, REM, ORD

Minimum length = 1

Minimum length = 1

Minimum length = 1

Minimum length = 1

Operations

(click to see Properties)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

sslcipher_servicegroup_binding

Binding object showing the servicegroup that can be bound to sslcipher.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ciphergroupname	<String>	Read-write	Name of the user-defined cipher group. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
servicegroup	<Boolean>	Read-write	Indicates that the cipher operation is to be performed on the named SSL service or service group.
servicename	<String>	Read-write	The name of the SSL service name to which the cipher-suite is to be bound. Minimum length = 1
service	<Boolean>	Read-write	Indicates that the cipher operation is to be performed on the named SSL service or service group.
cipherpriority	<Integer>	Read-write	Priority of the cipher to be added. Minimum value = 1 Maximum value = 1000
cipheroperation	<String>	Read-write	The operation that is performed when adding the cipher-suite.

Possible cipher operations are: ADD - Appends the given cipher-suite to the existing one configured for the virtual server. REM - Removes the given cipher-suite from the existing one configured for the virtual server. ORD - Overrides the current configured cipher-suite for the virtual server with the given cipher-suite.

Default value: 0

Possible values = ADD, REM, ORD

Minimum length = 1

Minimum length = 1

Operations

(click to see Properties)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

sslcipher_sslciphersuite_binding

Binding object showing the sslciphersuite that can be bound to sslcipher.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ciphgrpals	<String>	Read-write	A cipher-suite can consist of an individual cipher name, the system predefined cipher-alias name, or user defined cipher-group name. Minimum length = 1
cipherpriority	<Integer>	Read-write	This indicates priority assigned to the particular cipher. Minimum value = 1
cipheroperation	<String>	Read-write	The operation that is performed when adding the cipher-suite.

Possible cipher operations are: ADD - Appends the given cipher-suite to the existing one configured for the virtual server. REM - Removes the given cipher-suite from the existing one configured for the virtual server. ORD - Overrides the current configured cipher-suite for the virtual server with the given cipher-suite.

Default value: 0

Possible values = ADD, REM, ORD

Minimum length = 1

Operations

(click to see Properties)

- ADD
- GET
- GET (ALL)
- COUNT

- DELETE

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/sslcipher_sslciphersuite_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"sslcipher_sslciphersuite_binding":{

"ciphergroupname":<String_value>,

"cipheroperation":<String_value>,

"ciphgrpals":<String_value>,

"ciphername":<String_value>,

"cipherpriority":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcipher_sslciphersuite_binding/ ciphergroupname_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/ config/sslcipher_sslciphersuite_binding/ ciphergroupname_value<String> ? **args=ciphername: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcipher_sslciphersuite_binding/ ciphergroupname_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/

config/sslcipher_sslciphersuite_binding/ ciphergroupname_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of sslcipher_sslciphersuite_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/sslcipher_sslciphersuite_binding/ ciphergroupname_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the sslcipher_sslciphersuite_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslcipher_sslciphersuite_binding": [ {

"ciphgrpals":<String_value>,

"cipherpriority":<Integer_value>,

"cipheroperation":<String_value>,

"ciphername":<String_value>,

"ciphergroupname":<String_value>,

"description":<String_value>
```

```
}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcipher_sslciphersuite_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/sslcipher_sslciphersuite_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslcipher_sslciphersuite_binding": [ {

"ciphgrpals":<String_value>,

"cipherpriority":<Integer_value>,

"cipheroperation":<String_value>,

"ciphername":<String_value>,

"ciphergroupname":<String_value>,
```

```
"description":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcipher_sslciphersuite_binding/ciphergroupname_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"sslcipher_sslciphersuite_binding": [ { "__count": "#no"} ] }
```

sslcipher_sslprofile_binding

Binding object showing the sslprofile that can be bound to sslcipher.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ciphergroupname	<String>	Read-write	Name of the user-defined cipher group. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
description	<String>	Read-write	Cipher suite description.
cipherpriority	<Integer>	Read-write	Priority of the cipher to be added. Minimum value = 1 Maximum value = 1000
cipheroperation	<String>	Read-write	The operation that is performed when adding the cipher-suite.

Possible cipher operations are: ADD - Appends the given cipher-suite to the existing one configured for the virtual server. REM - Removes the given cipher-suite from the existing one configured for the virtual server. ORD - Overrides the current configured cipher-suite for the virtual server with the given cipher-suite.

Default value: 0

Possible values = ADD, REM, ORD

Minimum length = 1

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcipher_sslprofile_binding/ ciphergroupname_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/ config/sslcipher_sslprofile_binding/ ciphergroupname_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of sslcipher_sslprofile_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/sslcipher_sslprofile_binding/ ciphergroupname_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the sslcipher_sslprofile_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslcipher_sslprofile_binding": [ {

"ciphergroupname":<String_value>,

"description":<String_value>,

"cipherpriority":<Integer_value>,

"cipheroperation":<String_value>,

"sslprofile":<String_value>,

"ciphgrpals":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcipher_sslprofile_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/sslcipher_sslprofile_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslcipher_sslprofile_binding": [ {

"ciphergroupname":<String_value>,

"description":<String_value>,

"cipherpriority":<Integer_value>,

"cipheroperation":<String_value>,

"sslprofile":<String_value>,

"ciphgrpals":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcipher_sslprofile_binding/ciphergroupname_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"sslcipher_sslprofile_binding": [ { "__count": "#no"} ] }
```

sslcipher_sslvserver_binding

Binding object showing the sslvserver that can be bound to sslcipher.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
vservername	<String>	Read-write	The name of the SSL virtual server to which the cipher-suite is to be bound. Minimum length = 1
ciphergroupname	<String>	Read-write	Name of the user-defined cipher group. Minimum length = 1
vserver	<Boolean>	Read-write	Select the -vServer flag when the cipher operation is performed on an SSL virtual server.

Note: By default the bind ssl cipher command internally assumes the flag of -vServer argument. Hence, while working with the SSL vserver, you need not specify this flag.

Possible cipher operations are: ADD - Appends the given cipher-suite to the existing one configured for the virtual server. REM - Removes the given cipher-suite from the existing one configured for the virtual server. ORD - Overrides the current configured cipher-suite for the virtual server with the given cipher-suite.

Default value: 0

Possible values = ADD, REM, ORD

Minimum value = 1

Maximum value = 1000

Minimum length = 1

Operations

(click to see Properties)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

sslciphersuite

Configuration for ciphersuite resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ciphername	<String>	Read-write	Name of the cipher suite for which to show detailed information.
description	<String>	Read-only	Cipher suite description.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslciphersuite

Query-parameters:

attrs

http:// <netscaler-ip-address> /nitro/v1/config/sslciphersuite? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter

http:// <netscaler-ip-address> /nitro/v1/config/sslciphersuite? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of sslciphersuite resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view

http:// <netscaler-ip-address> /nitro/v1/config/sslciphersuite? **view=summary**

Use this query-parameter to get the summary output of sslciphersuite resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination

http:// <netscaler-ip-address> /nitro/v1/config/sslciphersuite? **pagesize=#no;pageno=#no**

Use this query-parameter to get the sslciphersuite resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "sslciphersuite": [ {

"ciphername":<String_value>,

"description":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslciphersuite/ ciphername_value<String>

Query-parameters:

attrs

http:// <netscaler-ip-address> /nitro/v1/config/sslciphersuite/ ciphername_value<String> ?**attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view

http:// <netscaler-ip-address> /nitro/v1/config/sslciphersuite/ ciphername_value<String> ? **view=summary**

Use this query-parameter to get the summary output of sslciphersuite resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslciphersuite": [ {

"ciphername":<String_value>,

"description":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslciphersuite? **count=yes**

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "sslciphersuite": [ { "__count": "#no"} ] }
```

sslcrl

Configuration for Certificate Revocation List resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
crlname	<String>	Read-write	Name for the Certificate Revocation List (CRL). Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the CRL is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my crl" or 'my crl'). Minimum length = 1
crlpath	<String>	Read-write	Path to the CRL file. /var/netscaler/ssl/ is the default path. Minimum length = 1
inform	<String>	Read-write	Input format of the CRL file. The two formats supported on the appliance are: PEM - Privacy Enhanced Mail. DER - Distinguished Encoding Rule.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: PEM Possible values = DER, PEM
refresh	<String>	Read-write	Set CRL auto refresh. Possible values = ENABLED, DISABLED
cacert	<String>	Read-write	CA certificate that has issued the CRL. Required if CRL Auto Refresh is selected. Install the CA certificate on the appliance before adding the CRL. Minimum length = 1
method	<String>	Read-write	Method for CRL refresh. If LDAP is selected, specify the method, CA certificate, base DN, port, and LDAP server name. If HTTP is selected, specify the CA certificate, method, URL, and port. Cannot be changed after a CRL is added. Possible values = HTTP, LDAP
server	<String>	Read-write	IP address of the LDAP server from

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			which to fetch the CRLs. Minimum length = 1
url	<String>	Read-write	URL of the CRL distribution point.
port	<Integer>	Read-write	Port for the LDAP server. Minimum value = 1
basedn	<String>	Read-write	Base distinguished name (DN), which is used in an LDAP search to search for a CRL. Citrix recommends searching for the Base DN instead of the Issuer Name from the CA certificate, because the Issuer Name field might not exactly match the LDAP directory structure's DN. Minimum length = 1
scope	<String>	Read-write	Extent of the search operation on the LDAP server. Available settings function as follows: One - One level below Base DN. Base - Exactly the same level as Base DN.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: One Possible values = Base, One
interval	<String>	Read-write	CRL refresh interval. Use the NONE setting to unset this parameter. Possible values = MONTHLY, WEEKLY, DAILY, NOW, NONE
day	<Integer>	Read-write	Day on which to refresh the CRL, or, if the Interval parameter is not set, the number of days after which to refresh the CRL. If Interval is set to MONTHLY, specify the date. If Interval is set to WEEKLY, specify the day of the week (for example, Sun=0 and Sat=6). This parameter is not applicable if the Interval is set to DAILY. Minimum value = 0 Maximum value = 31
time	<String>	Read-write	Time, in hours (1-24) and minutes (1-60),

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			at which to refresh the CRL.
binddn	<String>	Read-write	Bind distinguished name (DN) to be used to access the CRL object in the LDAP repository if access to the LDAP repository is restricted or anonymous access is not allowed. Minimum length = 1
password	<String>	Read-write	Password to access the CRL in the LDAP repository if access to the LDAP repository is restricted or anonymous access is not allowed. Minimum length = 1
binary	<String>	Read-write	Set the LDAP-based CRL retrieval mode to binary. Default value: NO Possible values = YES, NO
cacertfile	<String>	Read-write	Name of and, optionally, path to the CA certificate file. /nsconfig/ssl/ is the default path.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum length = 63
cakeyfile	<String>	Read-write	Name of and, optionally, path to the CA key file. /nsconfig/ssl/ is the default path. Maximum length = 63
indexfile	<String>	Read-write	Name of and, optionally, path to the file containing the serial numbers of all the certificates that are revoked. Revoked certificates are appended to the file. /nsconfig/ssl/ is the default path. Maximum length = 63
revoke	<String>	Read-write	Name of and, optionally, path to the certificate to be revoked. /nsconfig/ssl/ is the default path. Maximum length = 63
gencrl	<String>	Read-write	Name of and, optionally, path to the CRL file to be generated. The list of certificates that have been revoked is obtained from the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			index file. /nsconfig/ssl/ is the default path. Maximum length = 63
flags	<Integer>	Read-only	CRL status flag.
lastupdatetime	<Integer>	Read-only	Last CRL refresh time.
version	<Integer>	Read-only	CRL version.
signaturealgo	<String>	Read-only	Signature algorithm.
issuer	<String>	Read-only	Issuer name.
lastupdate	<String>	Read-only	Last update time.
nextupdate	<String>	Read-only	Next update time.
daystoexpiration	<Integer>	Read-only	Number of days remaining for the CRL to expire.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- CREATE
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET

- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcrl **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"sslcrl":{

<b>"crlname":<String_value>,
```

```
</b><b>"crlpath":<String_value>,

</b>"inform":<String_value>,

"refresh":<String_value>,

"cacert":<String_value>,

"method":<String_value>,

"server":<String_value>,

"url":<String_value>,

"port":<Integer_value>,

"basedn":<String_value>,

"scope":<String_value>,

"interval":<String_value>,

"day":<Integer_value>,

"time":<String_value>,

"binddn":<String_value>,

"password":<String_value>,

"binary":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

CREATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcrl? **action=create HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"sslcrl":{

<b>"cacertfile":<String_value>,

</b><b>"cakeyfile":<String_value>,

</b><b>"indexfile":<String_value>,

</b>"revoke":<String_value>,

"gencrl":<String_value>,

"password":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcrl/ crlname_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcrl **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"sslcrl":{

<b>"crlname":<String_value>,

</b>"refresh":<String_value>,

"cacert":<String_value>,

"server":<String_value>,

"method":<String_value>,

"url":<String_value>,

"port":<Integer_value>,

"basedn":<String_value>,

"scope":<String_value>,

"interval":<String_value>,

"day":<Integer_value>,

"time":<String_value>,

"binddn":<String_value>,

"password":<String_value>,

"binary":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcrl? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"sslcrl":{

<b>"crlname":<String_value>,

</b>"refresh":true,

"cacert":true,

"server":true,

"method":true,

"url":true,

"port":true,

"basedn":true,

"scope":true,

"interval":true,

"day":true,

"time":true,
```

```
"binddn":true,

"password":true,

"binary":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcrl **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/sslcrl? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/sslcrl? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of sslcrl resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/sslcrl? **view=summary**

Use this query-parameter to get the summary output of sslcrl resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/sslcrl? **pagesize=#no;pageno=#no**

Use this query-parameter to get the sslcrl resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "sslcrl": [ {

"crlname":<String_value>,

"crlpath":<String_value>,

"inform":<String_value>,

"cacert":<String_value>,

"refresh":<String_value>,

"scope":<String_value>,

"server":<String_value>,

"port":<Integer_value>,

"url":<String_value>,

"method":<String_value>,

"basedn":<String_value>,

"interval":<String_value>,

"day":<Integer_value>,

"time":<String_value>,

"binddn":<String_value>,

"password":<String_value>,
```

```
"flags":<Integer_value>,

"lastupdatetime":<Integer_value>,

"version":<Integer_value>,

"signaturealgo":<String_value>,

"issuer":<String_value>,

"lastupdate":<String_value>,

"nextupdate":<String_value>,

"binary":<String_value>,

"daystoexpiration":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcrl/ crlname_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/sslcrl/ crlname_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/sslcrl/ crlname_value<String> ? **view=summary**

Use this query-parameter to get the summary output of sslcrl resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslcrl": [ {

"crlname":<String_value>,

"crlpath":<String_value>,

"inform":<String_value>,

"cacert":<String_value>,

"refresh":<String_value>,

"scope":<String_value>,

"server":<String_value>,

"port":<Integer_value>,

"url":<String_value>,

"method":<String_value>,

"basedn":<String_value>,

"interval":<String_value>,

"day":<Integer_value>,

"time":<String_value>,

"binddn":<String_value>,
```

```
"password":<String_value>,

"flags":<Integer_value>,

"lastupdatetime":<Integer_value>,

"version":<Integer_value>,

"signaturealgo":<String_value>,

"issuer":<String_value>,

"lastupdate":<String_value>,

"nextupdate":<String_value>,

"binary":<String_value>,

"daystoexpiration":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcrl? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "sslcrl": [ { "__count": "#no"} ] }
```

sslcrl_binding

Binding object which returns the resources bound to sslcrl.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
crlname	<String>	Read-write	Name of the CRL for which to show detailed information. Minimum length = 1
sslcrl_serialnumber_binding	<sslcrl_serialnumber_binding[]>	Read-only	serialnumber that can be bound to sslcrl.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcrl_binding/ crlname_value<String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "sslcrl_binding": [ {

"crlname":<String_value>,

"sslcrl_serialnumber_binding":<sslcrl_serialnumber_binding[]_value>
```

```
}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcrl_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/sslcrl_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "sslcrl_binding": [ {

"crlname":<String_value>,

"sslcrl_serialnumber_binding":<sslcrl_serialnumber_binding[]_value>

}]}
```

sslcrl_serialnumber_binding

Binding object showing the serialnumber that can be bound to sslcrl.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
crlname	<String>	Read-write	Name of the CRL for which to show detailed information. Minimum length = 1
number	<String>	Read-write	Certificate Serial number.
date	<String>	Read-only	Certificate Revocation date.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.
- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcrl_serialnumber_binding/ crlname_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ sslcrl_serialnumber_binding/ crlname_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of sslcrl_serialnumber_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/sslcrl_serialnumber_binding/ crlname_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the sslcrl_serialnumber_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslcrl_serialnumber_binding": [ {

"crlname":<String_value>,

"number":<String_value>,

"date":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcrl_serialnumber_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/sslcrl_serialnumber_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslcrl_serialnumber_binding": [ {

"crlname":<String_value>,
```

```
"number":<String_value>,

"date":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcrl_serialnumber_binding/ crlname_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"sslcrl_serialnumber_binding": [ { "__count": "#no"} ] }
```

sslcrlfile

Configuration for Imported crl files resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name to assign to the imported CRL

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			file. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my file" or 'my file'). Minimum length = 1 Maximum length = 31
src	<String>	Read-write	URL specifying the protocol, host, and path, including file name to the CRL file to be imported. For example, http://www.example.com/crl_file. NOTE: The import fails if the object to be imported is on

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			an HTTPS server that requires client certificate authentication for access, and the issuer certificate of the HTTPS server is not present in the specific path on NetScaler to authenticate the HTTPS server. Minimum length = 1 Maximum length = 2047
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- IMPORT
- DELETE
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

IMPORT

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcrlfile? **action=Import HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"sslcrlfile":{

<b>"name":<String_value>,

</b><b>"src":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcrlfile **Query-parameters: args= name:<String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcrlfile **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/sslcrlfile? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/sslcrlfile? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of sslcrlfile resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/sslcrlfile? **view=summary**

Use this query-parameter to get the summary output of sslcrlfile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/sslcrlfile? **pagesize=#no;pageno=#no**

Use this query-parameter to get the sslcrlfile resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "sslcrlfile": [ {

"name":<String_value>,

"src":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcrlfile? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "sslcrlfile": [ { "__count": "#no"} ] }
```

ssldefaultprofile

Configuration for 0 resource.

Operations

- CONVERT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

CONVERT

URL: http:// <netscaler-ip-address> /nitro/v1/config/ssldefaultprofile? **action=convert**

HTTP Method: POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"ssldefaultprofile":{

}}
```

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

ssldhfile

Configuration for dh imported file resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name to assign to the imported DH file. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@),

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			equals (=), and hyphen (-) characters. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my file" or 'my file'). Minimum length = 1 Maximum length = 31
src	<String>	Read-write	URL specifying the protocol, host, and path, including file name, to the DH file to be imported. For example, http://www.example.com/dh_file. NOTE: The import fails if the object to be imported is on an HTTPS server that requires client certificate authentication for access, and the issuer certificate of the HTTPS server is not present in the specific path on

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			NetScaler to authenticate the HTTPS server. Minimum length = 1 Maximum length = 2047
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- IMPORT
- DELETE
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

IMPORT

URL: http:// <netscaler-ip-address> /nitro/v1/config/ssldhfile? **action=Import HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"ssldhfile":{

<b>"name":<String_value>,

</b><b>"src":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/ssldhfile **Query-parameters: args= name:<String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/ssldhfile **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/ssldhfile? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/ssldhfile? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of ssldhfile resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/ssldhfile? **view=summary**

Use this query-parameter to get the summary output of ssldhfile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/ssldhfile? **pagesize=#no;pageno=#no**

Use this query-parameter to get the ssldhfile resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "ssldhfile": [ {

"name":<String_value>,

"src":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/ssldhfile? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "ssldhfile": [ { "__count": "#no"} ] }
```

ssldhparam

Configuration for dh Parameter resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
dhfile	<String>	Read-write	Name of and, optionally, path to the DH key file. /nsconfig/ssl/ is the default path. Maximum length = 63
bits	<Integer>	Read-write	Size, in bits, of the DH key being generated. Minimum value = 512 Maximum value = 2048
gen	<String>	Read-write	Random number required for generating the DH key. Required as part of the DH key generation algorithm. Default value: 2 Possible values = 2, 5

Operations

(click to see Properties)

- CREATE

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

CREATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/ssldhparam? **action=create HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"ssldhparam":{

<b>"dhfile":<String_value>,

</b>"bits":<Integer_value>,
```

```
"gen":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

ssldtlsprofile

Configuration for DTLS profile resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the DTLS profile. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@),equals sign (=), and hyphen (-) characters. Cannot be changed after the profile is created. Minimum length = 1 Maximum length = 127
pmtudiscovery	<String>	Read-write	Source for the maximum record

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			size value. If ENABLED, the value is taken from the PMTU table. If DISABLED, the value is taken from the profile. Default value: DISABLED Possible values = ENABLED, DISABLED
maxrecordsize	<Integer>	Read-write	Maximum size of records that can be sent if PMTU is disabled. Default value: 1459 Minimum value = 250 Maximum value = 1459
maxretrytime	<Integer>	Read-write	Wait for the specified time, in seconds, before resending the request. Default value: 3
helloverifyrequest	<String>	Read-write	Send a Hello Verify request to validate the client. Default value: ENABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ENABLED, DISABLED
terminatesession	<String>	Read-write	Terminate the session if the message authentication code (MAC) of the client and server do not match. Default value: DISABLED Possible values = ENABLED, DISABLED
maxpacketsize	<Integer>	Read-write	Maximum number of packets to reassemble. This value helps protect against a fragmented packet attack. Default value: 120 Minimum value = 0 Maximum value = 86400
maxholdqlen	<Integer>	Read-write	Maximum number of datagrams that can be queued at DTLS layer for processing. Default value: 32 Minimum value = 32

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum value = 65535
maxbadmacignorecount	<Integer>	Read-write	Maximum number of bad MAC errors to ignore for a connection prior disconnect. Disabling parameter terminateSession terminates session immediately when bad MAC is detected in the connection. Default value: 100 Minimum value = 1 Maximum value = 65535
initialretrytimeout	<Integer>	Read-write	Initial time out value to retransmit the last flight sent from the NetScaler. Default value: 3 Minimum value = 1 Maximum value = 3
builtin	<String[]>	Read-only	Flag to determine whether dtls profile is built-in or not. Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
feature	<String>	Read-only	The feature to be checked while applying this config.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/ssldtlsprofile **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"ssldtlsprofile":{

<b>"name":<String_value>,

</b>"pmtudiscovery":<String_value>,

"maxrecordsize":<Integer_value>,

"maxretrytime":<Integer_value>,

"helloverifyrequest":<String_value>,

"terminatesession":<String_value>,

"maxpacketsize":<Integer_value>,

"maxholdqlen":<Integer_value>,

"maxbadmacignorecount":<Integer_value>,

"initialretrytimeout":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/ssldtlsprofile/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/ssldtlsprofile **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"ssldtlsprofile":{

<b>"name":<String_value>,

</b>"pmtudiscovery":<String_value>,

"maxrecordsize":<Integer_value>,

"maxretrytime":<Integer_value>,

"helloverifyrequest":<String_value>,

"terminatesession":<String_value>,
```

```
"maxpacketsize":<Integer_value>,

"maxholdqlen":<Integer_value>,

"maxbadmacignorecount":<Integer_value>,

"initialretrytimeout":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/ssldtlsprofile? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"ssldtlsprofile":{

<b>"name":<String_value>,

</b>"pmtudiscovery":true,

"maxrecordsize":true,

"maxretrytime":true,

"helloverifyrequest":true,

"terminatesession":true,
```

```
"maxpacketsize":true,

"maxholdqlen":true,

"maxbadmacignorecount":true,

"initialretrytimeout":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/ssldtlsprofile **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/ssldtlsprofile? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/ssldtlsprofile? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of ssldtlsprofile resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/ssldtlsprofile? **view=summary**

Use this query-parameter to get the summary output of ssldtlsprofile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/ssldtlsprofile? **pagesize=#no;pageno=#no**

Use this query-parameter to get the ssldtlsprofile resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "ssldtlsprofile": [ {

"name":<String_value>,

"pmtudiscovery":<String_value>,

"maxrecordsize":<Integer_value>,

"maxretrytime":<Integer_value>,

"helloverifyrequest":<String_value>,

"terminatesession":<String_value>,

"maxpacketsize":<Integer_value>,

"initialretrytimeout":<Integer_value>,

"maxholdqlen":<Integer_value>,

"maxbadmacignorecount":<Integer_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/ssldtlsprofile/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/ssldtlsprofile/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/ssldtlsprofile/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of ssldtlsprofile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "ssldtlsprofile": [ {

"name":<String_value>,

"pmtudiscovery":<String_value>,

"maxrecordsize":<Integer_value>,
```

```
"maxretrytime":<Integer_value>,

"helloverifyrequest":<String_value>,

"terminatesession":<String_value>,

"maxpacketsize":<Integer_value>,

"initialretrytimeout":<Integer_value>,

"maxholdqlen":<Integer_value>,

"maxbadmacignorecount":<Integer_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/ssldtlsprofile? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "ssldtlsprofile": [ { "__count": "#no"} ] }
```

sslecdsakey

Configuration for ecdsa key resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
keyfile	<String>	Read-write	Name for and, optionally, path to the ECDSA key file. /nsconfig/ssl/ is the default path. Maximum length = 63
curve	<String>	Read-write	Curve id to generate ECDSA key. Only P_256 and P_384 are supported. Default value: FIPSEXP_F4 Possible values = P_256, P_384
keyform	<String>	Read-write	Format in which the ECDSA key file is stored on the appliance. Default value: PEM Possible values = DER, PEM
des	<Boolean>	Read-write	Encrypt the generated ECDSA key by using the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			DES algorithm. On the command line, you are prompted to enter the pass phrase (password) that is used to encrypt the key.
des3	<Boolean>	Read-write	Encrypt the generated ECDSA key by using the Triple-DES algorithm. On the command line, you are prompted to enter the pass phrase (password) that is used to encrypt the key.
aes256	<Boolean>	Read-write	Encrypt the generated ECDSA key by using the AES algorithm.
password	<String>	Read-write	Pass phrase to use for encryption if DES or DES3 option is selected. Minimum length = 1 Maximum length = 31
pkcs8	<Boolean>	Read-write	Create the private key in PKCS#8 format.

Operations

(click to see Properties)

- CREATE

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

CREATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslecdsakey? **action=create HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"sslecdsakey":{

<b>"keyfile":<String_value>,

</b><b>"curve":<String_value>,

</b>"keyform":<String_value>,

"des":<Boolean_value>,

"des3":<Boolean_value>,

"aes256":<Boolean_value>,

"password":<String_value>,

"pkcs8":<Boolean_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

sslechconfig

Configuration for ech config resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
echconfigname	<String>	Read-write	The ECH config name configured. Minimum length = 1
echcipher	<String>	Read-write	The supported cipher suite that encrypts

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			the client Hello Message. Possible values = AES128-GCM-HKDFSHA256, AES128-GCM-HKDFSHA384, AES128-GCM-HKDFSHA512, AES256-GCM-HKDFSHA256, AES256-GCM-HKDFSHA384, AES256-GCM-HKDFSHA512, CHACHA20-POLY1305-HKDFSHA256, CHACHA20-POLY1305-HKDFSHA384, CHACHA20-POLY1305-HKDFSHA512
hpkekeyname	<String>	Read-write	The name of the configured HPKE key. Minimum length = 1
echpublicname	<String>	Read-write	The public name of ech config means FQDN or any string. Minimum length = 1
echconfigid	<Integer>	Read-write	The config id of the ech config.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum value = 0 Maximum value = 255
version	<Integer>	Read-write	The version of ECH for which this configuration is used. Default value: 65037
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of

creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslechconfig **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"sslechconfig":{

<b>"echconfigname":<String_value>,

</b><b>"echcipher":<String_value>,

</b><b>"hpkekeyname":<String_value>,

</b><b>"echpublicname":<String_value>,

</b><b>"echconfigid":<Integer_value>,

</b>"version":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslechconfig/ echconfigname_value<String>
HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslechconfig **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/sslechconfig? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/sslechconfig? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of sslechconfig resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/sslechconfig? **view=summary**

Use this query-parameter to get the summary output of sslechconfig resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/sslechconfig? **pagesize=#no;pageno=#no**

Use this query-parameter to get the sslechconfig resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "sslechconfig": [ {

"echconfigname":<String_value>,

"echcipher":<String_value>,

"hpkekeyname":<String_value>,

"version":<Integer_value>,

"echpublicname":<String_value>,

"echconfigid":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslechconfig/ echconfigname_value<String>
Query-parameters: attrs http:// <netscaler-ip-address> /nitro/v1/config/sslechconfig/ echconfigname_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/sslechconfig/ echconfigname_value<String> ? **view=summary**

Use this query-parameter to get the summary output of sslechconfig resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslechconfig": [ {

"echconfigname":<String_value>,

"echcipher":<String_value>,

"hpkekeyname":<String_value>,

"version":<Integer_value>,

"echpublicname":<String_value>,

"echconfigid":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslechconfig? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "sslechconfig": [ { "__count": "#no"} ] }
```

sslfips

Configuration for fips resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
inithsm	<String>	Read-write	FIPS initialization level. The appliance currently supports Level-2 (FIPS 140-2). Possible values = Level-2
sopassword	<String>	Read-write	Security officer password that will be in effect after you

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			have configured the HSM. Minimum length = 1
oldsopassword	<String>	Read-write	Old password for the security officer. Minimum length = 1
userpassword	<String>	Read-write	The Hardware Security Module's (HSM) User password. Minimum length = 1
hsmlabel	<String>	Read-write	Label to identify the Hardware Security Module (HSM). Minimum length = 1
fipsfw	<String>	Read-write	Path to the FIPS firmware file. Minimum length = 1
erasedata	<String>	Read-only	Erase data. Default value: FIPS_ERASE Minimum length = 1
serial	<Integer>	Read-only	FIPS card serial number.
majorversion	<Integer>	Read-only	Firmware major version.
minorversion	<Integer>	Read-only	Firmware minor version.
fipshwmajorversion	<Integer>	Read-only	FIPS card hardware major version.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
fipshwminorversion	<Integer>	Read-only	FIPS card hardware minor version.
fipshwversionstring	<String>	Read-only	FIPS card hardware extended version string.
flashmemorytotal	<Integer>	Read-only	Total size of the flash memory on card.
flashmemoryfree	<Integer>	Read-only	Total size of free flash memory.
sramtotal	<Integer>	Read-only	Total size of the SRAM memory on card.
sramfree	<Integer>	Read-only	Total size of free SRAM memory.
status	<Integer>	Read-only	Status.
flag	<Integer>	Read-only	Internal Flags.
serialno	<String>	Read-only	FIPS card serial number.
model	<String>	Read-only	FIPS card model info.
state	<Integer>	Read-only	FIPS card state.
firmwarereleasedate	<String>	Read-only	FIPS card firmware revision date.
coresmax	<Integer>	Read-only	Maximum number of crypto cores present in the FIPS card.
coresenabled	<Integer>	Read-only	Number of crypto cores enabled in the FIPS card.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- UPDATE
- UNSET
- RESET
- GET (ALL)
- CHANGE

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslfips **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"sslfips":{

<b>"inithsm":<String_value>,

</b><b>"sopassword":<String_value>,

</b><b>"oldsopassword":<String_value>,

</b><b>"userpassword":<String_value>,

</b>"hsmlabel":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslfips? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"sslfips":{

"hsmlabel":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

RESET

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslfips? **action=reset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"sslfips":{

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

CHANGE

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslfips? **action=update HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"sslfips":{

<b>"fipsfw":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslfips **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "sslfips": [ {

"inithsm":<String_value>,

"sopassword":<String_value>,

"userpassword":<String_value>,

"oldsopassword":<String_value>,

"erasedata":<String_value>,
```

```
"hsmlabel":<String_value>,

"serial":<Integer_value>,

"majorversion":<Integer_value>,

"minorversion":<Integer_value>,

"fipshwmajorversion":<Integer_value>,

"fipshwminorversion":<Integer_value>,

"fipshwversionstring":<String_value>,

"flashmemorytotal":<Integer_value>,

"flashmemoryfree":<Integer_value>,

"sramtotal":<Integer_value>,

"sramfree":<Integer_value>,

"status":<Integer_value>,

"flag":<Integer_value>,

"serialno":<String_value>,

"model":<String_value>,

"state":<Integer_value>,

"firmwarereleasedate":<String_value>,

"coresmax":<Integer_value>,

"coresenabled":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

sslfipskey

Configuration for FIPS key resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
fipskeyname	<String>	Read-write	Name for the FIPS key. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the FIPS key is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my fipskey" or 'my fipskey').

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum length = 1
keytype	<String>	Read-write	Only RSA key and ECDSA Key are supported. Default value: RSA Possible values = RSA, ECDSA
exponent	<String>	Read-write	Exponent value for the FIPS key to be created. Available values function as follows: 3=3 (hexadecimal) F4=10001 (hexadecimal). Default value: 3 Possible values = 3, F4
modulus	<Integer>	Read-write	Modulus, in multiples of 64, of the FIPS key to be created. Minimum value = 0 Maximum value = 4096
curve	<String>	Read-write	Only p_256 (prime256v1) and P_384 (secp384r1) are supported. Default value: P_256

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = P_256, P_384
key	<String>	Read-write	Name of and, optionally, path to the key file to be imported. /nsconfig/ssl/ is the default path. Minimum length = 1
inform	<String>	Read-write	Input format of the key file. Available formats are: SIM - Secure Information Management; select when importing a FIPS key. If the external FIPS key is encrypted, first decrypt it, and then import it. PEM - Privacy Enhanced Mail; select when importing a non-FIPS key. Default value: SIM Possible values = SIM, DER, PEM
wrapkeyname	<String>	Read-write	Name of the wrap key to use for importing the key. Required for

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			importing a non-FIPS key. Minimum length = 1
iv	<String>	Read-write	Initialization Vector (IV) to use for importing the key. Required for importing a non-FIPS key. Minimum length = 1
size	<Integer>	Read-only	Size.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- CREATE
- DELETE
- GET (ALL)
- GET
- COUNT
- IMPORT
- EXPORT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

CREATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslfipskey? **action=create HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"sslfipskey":{

<b>"fipskeyname":<String_value>,

</b><b>"keytype":<String_value>,

</b>"exponent":<String_value>,

"modulus":<Integer_value>,

"curve":<String_value>
```

```
}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslfipskey/ fipskeyname_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

IMPORT

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslfipskey? **action=Import HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"sslfipskey":{

<b>"fipskeyname":<String_value>,

</b><b>"key":<String_value>,

</b>"inform":<String_value>,

"wrapkeyname":<String_value>,
```

```
"iv":<String_value>,

"exponent":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

EXPORT

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslfipskey? **action=export HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"sslfipskey":{

<b>"fipskeyname":<String_value>,

</b><b>"key":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslfipskey **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/sslfipskey? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/sslfipskey? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of sslfipskey resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/sslfipskey? **view=summary**

Use this query-parameter to get the summary output of sslfipskey resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/sslfipskey? **pagesize=#no;pageno=#no**

Use this query-parameter to get the sslfipskey resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "sslfipskey": [ {

"fipskeyname":<String_value>,

"modulus":<Integer_value>,

"exponent":<String_value>,
```

```
"curve":<String_value>,

"keytype":<String_value>,

"size":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslfipskey/ fipskeyname_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/sslfipskey/ fipskeyname_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/sslfipskey/ fipskeyname_value<String> ? **view=summary**

Use this query-parameter to get the summary output of sslfipskey resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslfipskey": [ {

"fipskeyname":<String_value>,

"modulus":<Integer_value>,

"exponent":<String_value>,

"curve":<String_value>,

"keytype":<String_value>,

"size":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslfipskey? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "sslfipskey": [ { "__count": "#no"} ] }
```

sslfipssimsource

Configuration for FIPsSIM source resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
targetsecret	<String>	Read-write	Name of and, optionally, path to the target FIPS appliance's secret data. /nsconfig/ssl/ is the default path. Minimum length = 1
sourcesecret	<String>	Read-write	Name for and, optionally, path to the source FIPS appliance's secret data. /nsconfig/ssl/ is the default path. Minimum length = 1
certfile	<String>	Read-write	Name for and, optionally, path to the source FIPS appliance's certificate file. /nsconfig/ssl/ is the default path. Minimum length = 1

Operations

(click to see Properties)

- ENABLE
- INIT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ENABLE

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslfipssimsource? **action=enable HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"sslfipssimsource":{

<b>"targetsecret":<String_value>,

</b><b>"sourcesecret":<String_value>
```

```
</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

INIT

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslfipssimsource? **action=init HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"sslfipssimsource":{

<b>"certfile":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

sslfipssimtarget

Configuration for FIPS SIM Target resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
keyvector	<String>	Read-write	Name of and, optionally, path to the target FIPS appliance's key vector. /nsconfig/ssl/ is the default path. Minimum length = 1
sourcesecret	<String>	Read-write	Name of and, optionally, path to the source FIPS appliance's secret data. /nsconfig/ssl/ is the default path. Minimum length = 1
certfile	<String>	Read-write	Name of and, optionally, path to the source FIPS appliance's certificate file. /nsconfig/ssl/ is the default path. Minimum length = 1
targetsecret	<String>	Read-write	Name for and, optionally, path to the target FIPS appliance's secret data. The default input path for the secret data is /nsconfig/ssl/. Minimum length = 1

Operations

(click to see Properties)

- ENABLE

- INIT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ENABLE

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslfipssimtarget? **action=enable HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"sslfipssimtarget":{

<b>"keyvector":<String_value>,

</b><b>"sourcesecret":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

INIT

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslfipssimtarget? **action=init HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"sslfipssimtarget":{

<b>"certfile":<String_value>,

</b><b>"keyvector":<String_value>,

</b><b>"targetsecret":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

sslglobal_binding

Binding object which returns the resources bound to sslglobal.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
sslglobal_sslpolicy_binding	<sslglobal_sslpolicy_binding[]>	Read-write	sslpolicy that can be bound to sslglobal.

Operations

(click to see Properties)

- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslglobal_binding

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "sslglobal_binding": [ {

"sslglobal_sslpolicy_binding":<sslglobal_sslpolicy_binding[]_value>

}]}
```

sslglobal_sslpolicy_binding

Binding object showing the sslpolicy that can be bound to sslglobal.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
labelname	<String>	Read-write	Name of the virtual server or user-defined policy label to invoke if the policy evaluates to TRUE.
labeltype	<String>	Read-write	Type of policy label to invoke. Specify virtual server for a policy label associated with a virtual server, or policy label for a user-defined policy label. Possible values = vserver, service, policylabel
priority	<Integer>	Read-write	The priority of the policy binding.
globalbindtype	<String>	Read-write	. Default value: SYSTEM_GLOBAL Possible values = SYSTEM_GLOBAL, VPN_GLOBAL, RNAT_GLOBAL, APPFW_GLOBAL, TM_GLOBAL
policyname	<String>	Read-write	The name for the SSL policy.
gotopriorityexpression	<String>	Read-write	Expression or other value specifying the next policy to be evaluated if the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			current policy evaluates to TRUE. Specify one of the following values: * NEXT - Evaluate the policy with the next higher priority number. * END - End policy evaluation. * USE_INVOCATION_RESULT - Applicable if this policy invokes another policy label. If the final goto in the invoked policy label has a value of END, the evaluation stops. If the final goto is anything other than END, the current policy label performs a NEXT. * An expression that evaluates to a number. If you specify an expression, the number to which it evaluates determines the next policy to evaluate, as follows: * If the expression evaluates to a higher numbered priority, the policy with that priority is evaluated next. * If the expression evaluates to the priority of the current policy, the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			policy with the next higher numbered priority is evaluated next. * If the expression evaluates to a number that is larger than the largest numbered priority, policy evaluation ends. An UNDEF event is triggered if: * The expression is invalid. * The expression evaluates to a priority number that is numerically lower than the current policy's priority. * The expression evaluates to a priority number that is between the current policy's priority number (say, 30) and the highest priority number (say, 100), but does not match any configured priority number (for example, the expression evaluates to the number 85). This example assumes that the priority number increments by 10 for every successive policy, and therefore a priority number of

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			85 does not exist in the policy label. Default value: "END"
invoke	<Boolean>	Read-write	Invoke policies bound to a virtual server, service, or policy label. After the invoked policies are evaluated, the flow returns to the policy with the next priority.
type	<String>	Read-write	Global bind point to which the policy is bound. Possible values = CONTROL_OVERRIDE, CONTROL_DEFAULT, DATA_OVERRIDE, DATA_DEFAULT, HTTPQUIC_CONTROL_OVERRIDE, HTTPQUIC_CONTROL_DEFAULT, HTTPQUIC_DATA_OVERRIDE, HTTPQUIC_DATA_DEFAULT
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/sslglobal_sslpolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"sslglobal_sslpolicy_binding":{

"policyname":<String_value>,

"priority":<Integer_value>,

"gotopriorityexpression":<String_value>,

"type":<String_value>,

"invoke":<Boolean_value>,

"labeltype":<String_value>,

"labelname":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslglobal_sslpolicy_binding **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/sslglobal_sslpolicy_binding? **args=policyname: <String_value> ,type: <String_value> ,priority: <Integer_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslglobal_sslpolicy_binding **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/sslglobal_sslpolicy_binding? **args=type: <String_value>**

Use this query-parameter to get sslglobal_sslpolicy_binding resources based on additional properties.

filter http:// <netscaler-ip-address> /nitro/v1/config/sslglobal_sslpolicy_binding? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of sslglobal_sslpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/sslglobal_sslpolicy_binding? **pagesize=#no;pageno=#no**

Use this query-parameter to get the sslglobal_sslpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslglobal_sslpolicy_binding": [ {

"labelname":<String_value>,

"labeltype":<String_value>,
```

```
"priority":<Integer_value>,

"globalbindtype":<String_value>,

"policyname":<String_value>,

"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>,

"type":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslglobal_sslpolicy_binding? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "sslglobal_sslpolicy_binding": [ { "__count": "#no"} ] }
```

sslhpkekey

Configuration for HPKE key resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
hpkekeyname	<String>	Read-write	The name of the hpke key configured that is used to decrypt ECH. Minimum length = 1
file	<String>	Read-write	Name of the HPKE key file. Minimum length = 1 Maximum length = 255
dhkem	<String>	Read-write	Type of curve used for HPKE. Possible values = X_25519
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslhpkekey **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"sslhpkekey":{

<b>"hpkekeyname":<String_value>,

</b><b>"file":<String_value>,

</b><b>"dhkem":<String_value>
```

```
</b>}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslhpkekey/ hpkekeyname_value<String>
HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslhpkekey **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/sslhpkekey? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/sslhpkekey? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of sslhpkekey resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/sslhpkekey? **view=summary**

Use this query-parameter to get the summary output of sslhpkekey resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/sslhpkekey? **pagesize=#no;pageno=#no**

Use this query-parameter to get the sslhpkekey resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "sslhpkekey": [ {

"hpkekeyname":<String_value>,

"file":<String_value>,

"dhkem":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslhpkekey/ hpkekeyname_value<String>
Query-parameters: attrs http:// <netscaler-ip-address> /nitro/v1/config/sslhpkekey/ hpkekeyname_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/sslhpkekey/ hpkekeyname_value<String> ? **view=summary**

Use this query-parameter to get the summary output of sslhpkekey resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslhpkekey": [ {

"hpkekeyname":<String_value>,

"file":<String_value>,

"dhkem":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslhpkekey? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "sslhpkekey": [ { "__count": "#no"} ] }
```

sslhsmkey

Configuration for HSM key resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
hsmkeyname	<String>	Read-write	. Minimum length = 1
hsmtype	<String>	Read-write	Type of HSM. Default value: THALES Possible values = THALES, SAFENET, KEYVAULT
key	<String>	Read-write	Name of the key. optionally, for Thales, path to the HSM key file; /var/opt/nfast/kmdata/local/ is the default path. Applies

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			when HSMTYPE is THALES or KEYVAULT. Maximum length = 63
serialnum	<String>	Read-write	Serial number of the partition on which the key is present. Applies only to SafeNet HSM. Maximum length = 16
password	<String>	Read-write	Password for a partition. Applies only to SafeNet HSM. Minimum length = 1
keystore	<String>	Read-write	Name of keystore object representing HSM where key is stored. For example, name of keyvault object or azurekeyvault authentication object. Applies only to KEYVAULT type HSM. Minimum length = 1
state	<String>	Read-only	Current state of key. Possible values = Created, Access Token Unavailable, Unauthorized, Does not exist, Unreachable, Marked down, Key

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			operations successful, Key operations failed, Key operation throttled
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslhsmkey **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"sslhsmkey":{

<b>"hsmkeyname":<String_value>,

</b>"hsmtype":<String_value>,

"key":<String_value>,

"serialnum":<String_value>,

"password":<String_value>,

"keystore":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslhsmkey/ hsmkeyname_value<String>
Query-parameters: args=hsmtype: <String_value> ,serialnum: <String_value> ,password: <String_value>
get (all)
URL: http:// <netscaler-ip-address> /nitro/v1/config/sslhsmkey **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/sslhsmkey? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/sslhsmkey? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of sslhsmkey resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/sslhsmkey? **view=summary**

Use this query-parameter to get the summary output of sslhsmkey resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/sslhsmkey? **pagesize=#no;pageno=#no**

Use this query-parameter to get the sslhsmkey resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "sslhsmkey": [ {

"hsmkeyname":<String_value>,

"hsmtype":<String_value>,

"key":<String_value>,

"serialnum":<String_value>,

"keystore":<String_value>,

"state":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

get
URL: http:// <netscaler-ip-address> /nitro/v1/config/sslhsmkey/ hsmkeyname_value<String>
Query-parameters: attrs http:// <netscaler-ip-address> /nitro/v1/config/sslhsmkey/ hsmkeyname_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/sslhsmkey/ hsmkeyname_value<String> ? **view=summary**

Use this query-parameter to get the summary output of sslhsmkey resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslhsmkey": [ {

"hsmkeyname":<String_value>,

"hsmtype":<String_value>,

"key":<String_value>,

"serialnum":<String_value>,

"keystore":<String_value>,

"state":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

count
URL: http:// <netscaler-ip-address> /nitro/v1/config/sslhsmkey? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "sslhsmkey": [ { "__count": "#no"} ] }
```

sslkeyfile

Configuration for Imported ssl key files resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name to assign to the imported key file. Must begin with an ASCII alphanumeric or underscore(_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@),equals (=), and hyphen (-) characters. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my file" or 'my file').

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum length = 1 Maximum length = 31
src	<String>	Read-write	URL specifying the protocol, host, and path, including file name, to the key file to be imported. For example, http://www.example.com/key_file. NOTE: The import fails if the object to be imported is on an HTTPS server that requires client certificate authentication for access, and the issuer certificate of the HTTPS server is not present in the specific path on NetScaler to authenticate the HTTPS server. Minimum length = 1 Maximum length = 2047
password	<String>	Read-write	.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- IMPORT
- DELETE
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

IMPORT

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslkeyfile? **action=Import HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"sslkeyfile":{

<b>"name":<String_value>,

</b><b>"src":<String_value>,

</b>"password":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslkeyfile **Query-parameters: args= name:<String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslkeyfile **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/sslkeyfile? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/sslkeyfile? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of sslkeyfile resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/sslkeyfile? **view=summary**

Use this query-parameter to get the summary output of sslkeyfile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/sslkeyfile? **pagesize=#no;pageno=#no**

Use this query-parameter to get the sslkeyfile resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "sslkeyfile": [ {

"name":<String_value>,

"src":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

```
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslkeyfile? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "sslkeyfile": [ { "__count": "#no"} ] }
```

ssllogprofile

Configuration for SSL logging Profile resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	The name of the ssllogprofile. Minimum length = 1 Maximum length = 127
ssllogclauth	<String>	Read-write	log all SSL ClAuth events.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: DISABLED Possible values = ENABLED, DISABLED
ssllogclauthfailures	<String>	Read-write	log all SSL ClAuth error events. Default value: DISABLED Possible values = ENABLED, DISABLED
ssllogs	<String>	Read-write	log all SSL HS events. Default value: DISABLED Possible values = ENABLED, DISABLED
ssllogsfailures	<String>	Read-write	log all SSL HS error events. Default value: DISABLED Possible values = ENABLED, DISABLED
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- UPDATE
- UNSET
- DELETE
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/ssllogprofile **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"ssllogprofile":{

<b>"name":<String_value>,

</b>"ssllogclauth":<String_value>,

"ssllogclauthfailures":<String_value>,

"ssllogs":<String_value>,

"ssllogsfailures":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/ssllogprofile **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"ssllogprofile":{

<b>"name":<String_value>,

</b>"ssllogclauth":<String_value>,
```

```
"ssllogclauthfailures":<String_value>,

"sslloghs":<String_value>,

"sslloghsfailures":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/ssllogprofile? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"ssllogprofile":{

<b>"name":<String_value>,

</b>"ssllogclauth":true,

"ssllogclauthfailures":true,

"sslloghs":true,

"sslloghsfailures":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/ssllogprofile/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/ssllogprofile **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/ssllogprofile? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/ssllogprofile? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of ssllogprofile resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/ssllogprofile? **view=summary**

Use this query-parameter to get the summary output of ssllogprofile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/ssllogprofile? **pagesize=#no;pageno=#no**

Use this query-parameter to get the ssllogprofile resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "ssllogprofile": [ {

"name":<String_value>,

"ssllogclauth":<String_value>,

"ssllogclauthfailures":<String_value>,

"ssllloghs":<String_value>,

"ssllloghsfailures":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/ssllogprofile/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/ssllogprofile/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/ssllogprofile/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of ssllogprofile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "ssllogprofile": [ {

"name":<String_value>,

"ssllogclauth":<String_value>,

"ssllogclauthfailures":<String_value>,

"sslloghs":<String_value>,

"sslloghsfailures":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/ssllogprofile? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "ssllogprofile": [ { "__count": "#no"} ] }
```

sslocspresponder

Configuration for OCSP responser resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the OCSP responder. Cannot begin with a hash (#) or space character and must contain only ASCII alphanumeric, underscore (_), hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the responder is created. The following requirement applies

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my responder" or 'my responder'). Minimum length = 1 Maximum length = 127
url	<String>	Read-write	URL of the OCSP responder. Minimum length = 1 Maximum length = 127
cache	<String>	Read-write	Enable caching of responses. Caching of responses received from the OCSP responder enables faster responses to the clients and reduces the load on the OCSP responder. Default value: DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ENABLED, DISABLED
cachetimeout	<Integer>	Read-write	Timeout for caching the OCSP response. After the timeout, the Citrix ADC sends a fresh request to the OCSP responder for the certificate status. If a timeout is not specified, the timeout provided in the OCSP response applies. Default value: 1 Minimum value = 1 Maximum value = 43200
batchingdepth	<Integer>	Read-write	Number of client certificates to batch together into one OCSP request. Batching avoids overloading the OCSP responder. A value of 1 signifies that each request is queried independently. For a value greater than 1, specify a timeout (batching delay) to avoid inordinately delaying the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			processing of a single certificate. Minimum value = 1 Maximum value = 8
batchingdelay	<Integer>	Read-write	Maximum time, in milliseconds, to wait to accumulate OCSP requests to batch. Does not apply if the Batching Depth is 1. Minimum value = 1 Maximum value = 10000
resptimeout	<Integer>	Read-write	Time, in milliseconds, to wait for an OCSP response. When this time elapses, an error message appears or the transaction is forwarded, depending on the settings on the virtual server. Includes Batching Delay time. Minimum value = 100 Maximum value = 120000
ocspurlresolvetimeout	<Integer>	Read-write	Time, in milliseconds, to wait for an OCSP URL Resolution. When this time elapses, an

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			error message appears or the transaction is forwarded, depending on the settings on the virtual server. Minimum value = 100 Maximum value = 2000
respondercert	<String>	Read-write	. Minimum length = 1
trustresponder	<Boolean>	Read-write	A certificate to use to validate OCSP responses. Alternatively, if -trustResponder is specified, no verification will be done on the reponse. If both are omitted, only the response times (producedAt, lastUpdate, nextUpdate) will be verified.
producedattimeskew	<Integer>	Read-write	Time, in seconds, for which the Citrix ADC waits before considering the response as invalid. The response is considered invalid if the Produced At time stamp in the OCSP response exceeds or

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			precedes the current Citrix ADC clock time by the amount of time specified. Default value: 300 Minimum value = 0 Maximum value = 86400
signingcert	<String>	Read-write	Certificate-key pair that is used to sign OCSP requests. If this parameter is not set, the requests are not signed. Minimum length = 1
usenonce	<String>	Read-write	Enable the OCSP nonce extension, which is designed to prevent replay attacks. Possible values = YES, NO
insertclientcert	<String>	Read-write	Include the complete client certificate in the OCSP request. Possible values = YES, NO
httpmethod	<String>	Read-write	HTTP method used to send ocsp request. POST is the default httpmethod. If request length is > 255, POST wil be

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			used even if GET is set as httpMethod. Default value: POST Possible values = GET, POST
ocspaiarefcount	<Integer>	Read-only	No of CA certs referencing this AIA responder.
ocspipaddrstr	<String>	Read-only	DNS resolved IP address.
port	<Integer>	Read-only	Port number on which OCSP Server listens. Range 1 - 65535 * in CLI is represented as 65535 in NITRO API
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- FLUSH
- UPDATE
- UNSET
- GET (ALL)

- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslocspresponder **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"sslocspresponder":{

<b>"name":<String_value>,

</b><b>"url":<String_value>,

</b>"cache":<String_value>,

"cachetimeout":<Integer_value>,

"batchingdepth":<Integer_value>,

"batchingdelay":<Integer_value>,

"resptimeout":<Integer_value>,

"ocspurlresolvetimeout":<Integer_value>,

"respondercert":<String_value>,

"trustresponder":<Boolean_value>,

"producedattimeskew":<Integer_value>,

"signingcert":<String_value>,

"usenonce":<String_value>,

"insertclientcert":<String_value>,

"httpmethod":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslocspresponder/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

FLUSH

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslocspresponder? **action=flush HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"sslocspresponder":{

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslocspresponder **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"sslocspresponder":{

<b>"name":<String_value>,

</b>"url":<String_value>,

"cache":<String_value>,

"cachetimeout":<Integer_value>,

"batchingdepth":<Integer_value>,

"batchingdelay":<Integer_value>,

"resptimeout":<Integer_value>,

"ocspurlresolvetimeout":<Integer_value>,

"respondercert":<String_value>,

"trustresponder":<Boolean_value>,

"producedattimeskew":<Integer_value>,

"signingcert":<String_value>,

"usenonce":<String_value>,

"insertclientcert":<String_value>,

"httpmethod":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslocspresponder? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"sslocspresponder":{

<b>"name":<String_value>,

</b>"trustresponder":true,

"insertclientcert":true,

"cache":true,

"cachetimeout":true,

"batchingdepth":true,

"batchingdelay":true,

"resptimeout":true,

"ocspurlresolvetimeout":true,

"respondercert":true,

"producedattimeskew":true,

"signingcert":true,

"usenonce":true,

"httpmethod":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslocspresponder **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/sslocspresponder? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/sslocspresponder? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of sslocspresponder resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/sslocspresponder? **view=summary**

Use this query-parameter to get the summary output of sslocspresponder resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/sslocspresponder? **pagesize=#no;pageno=#no**

Use this query-parameter to get the sslocspresponder resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "sslocspresponder": [ {

"name":<String_value>,

"url":<String_value>,

"cache":<String_value>,

"cachetimeout":<Integer_value>,

"batchingdepth":<Integer_value>,

"batchingdelay":<Integer_value>,

"ocspurlresolvetimeout":<Integer_value>,

"resptimeout":<Integer_value>,

"producedattimeskew":<Integer_value>,

"respondercert":<String_value>,

"trustresponder":<Boolean_value>,

"signingcert":<String_value>,

"usenonce":<String_value>,

"insertclientcert":<String_value>,

"ocspaiarefcount":<Integer_value>,

"httpmethod":<String_value>,

"ocspipaddrstr":<String_value>,

"port":<Integer_value>,
```

```
"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslocspresponder/ name_value<String>
Query-parameters: attrs http:// <netscaler-ip-address> /nitro/v1/config/sslocspresponder/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/sslocspresponder/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of sslocspresponder resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslocspresponder": [ {

"name":<String_value>,
```

```
"url":<String_value>,

"cache":<String_value>,

"cachetimeout":<Integer_value>,

"batchingdepth":<Integer_value>,

"batchingdelay":<Integer_value>,

"ocspurlresolvetimeout":<Integer_value>,

"resptimeout":<Integer_value>,

"producedattimeskew":<Integer_value>,

"respondercert":<String_value>,

"trustresponder":<Boolean_value>,

"signingcert":<String_value>,

"usenonce":<String_value>,

"insertclientcert":<String_value>,

"ocspaiarefcount":<Integer_value>,

"httpmethod":<String_value>,

"ocspipaddrstr":<String_value>,

"port":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslocspresponder? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "sslocspresponder": [ { "__count": "#no"} ] }
```

sslparameter

Configuration for SSL parameter resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
quantumsize	<String>	Read-write	Amount of data to collect before the data is pushed to the crypto hardware for encryption. For large downloads, a larger quantum size better utilizes the crypto resources. Default value: 8192 Possible values = 4096, 8192, 16384

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
crlmemorysizemb	<Integer>	Read-write	Maximum memory size to use for certificate revocation lists (CRLs). This parameter reserves memory for a CRL but sets a limit to the maximum memory that the CRLs loaded on the appliance can consume. Default value: 256 Minimum value = 10 Maximum value = 1024
strictcachecks	<String>	Read-write	Enable strict CA certificate checks on the appliance. Default value: NO Possible values = YES, NO
ssltriggertimeout	<Integer>	Read-write	Time, in milliseconds, after which encryption is triggered for transactions that are not tracked on the Citrix ADC because their length is not known. There can be a delay of up to 10ms from the specified timeout value before the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			packet is pushed into the queue. Default value: 100 Minimum value = 1 Maximum value = 200
sendclosenotify	<String>	Read-write	Send an SSL Close-Notify message to the client at the end of a transaction. Default value: YES Possible values = YES, NO
encrypttriggerpktcount	<Integer>	Read-write	Maximum number of queued packets after which encryption is triggered. Use this setting for SSL transactions that send small packets from server to Citrix ADC. Default value: 45 Minimum value = 10 Maximum value = 50
denysslreneg	<String>	Read-write	Deny renegotiation in specified circumstances. Available settings function as follows:

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			* NO - Allow SSL renegotiation. * FRONTEND_CLIENT - Deny secure and nonsecure SSL renegotiation initiated by the client. * FRONTEND_CLIENTSERVER - Deny secure and nonsecure SSL renegotiation initiated by the client or the Citrix ADC during policy-based client authentication. * ALL - Deny all secure and nonsecure SSL renegotiation. * NONSECURE - Deny nonsecure SSL renegotiation. Allows only clients that support RFC 5746. Default value: ALL

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = NO, FRONTEND_CLIENT, FRONTEND_CLIENTSERVER, ALL, NONSECURE
insertionencoding	<String>	Read-write	Encoding method used to insert the subject or issuer's name in HTTP requests to servers. Default value: Unicode Possible values = Unicode, UTF-8
ocspcachesize	<Integer>	Read-write	Size, per packet engine, in megabytes, of the OCSP cache. A maximum of 10% of the packet engine memory can be assigned. Because the maximum allowed packet engine memory is 4GB, the maximum value that can be assigned to the OCSP cache is approximately 410 MB. Default value: 10 Minimum value = 0

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum value = 512
pushflag	<Integer>	Read-write	Insert PUSH flag into decrypted, encrypted, or all records. If the PUSH flag is set to a value other than 0, the buffered records are forwarded on the basis of the value of the PUSH flag. Available settings function as follows: 0 - Auto (PUSH flag is not set.) 1 - Insert PUSH flag into every decrypted record. 2 -Insert PUSH flag into every encrypted record. 3 - Insert PUSH flag into every decrypted and encrypted record. Minimum value = 0 Maximum value = 3
dropreqwithnohostheader	<String>	Read-write	Host header check for SNI enabled sessions. If this check is enabled and the HTTP request does not contain the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			host header for SNI enabled sessions(i.e vserver or profile bound to vserver has SNI enabled and 'Client Hello' arrived with SNI extension), the request is dropped. Default value: NO Possible values = YES, NO
snihttphostmatch	<String>	Read-write	Controls how the HTTP 'Host' header value is validated. These checks are performed only if the session is SNI enabled (i.e when vserver or profile bound to vserver has SNI enabled and 'Client Hello' arrived with SNI extension) and HTTP request contains 'Host' header. Available settings function as follows: CERT - Request is forwarded if the 'Host' value is covered

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			by the certificate used to establish this SSL session. Note: 'CERT' matching mode cannot be applied in TLS 1.3 connections established by resuming from a previous TLS 1.3 session. On these connections, 'STRICT' matching mode will be used instead. STRICT - Request is forwarded only if value of 'Host' header in HTTP is identical to the 'Server name' value passed in 'Client Hello' of the SSL connection. NO - No validation is performed on the HTTP 'Host' header value.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: CERT Possible values = NO, CERT, STRICT
pushenctriggertimeout	<Integer>	Read-write	PUSH encryption trigger timeout value. The timeout value is applied only if you set the Push Encryption Trigger parameter to Timer in the SSL virtual server settings. Default value: 1 Minimum value = 1 Maximum value = 200
cryptodevdisablelimit	<Integer>	Read-write	Limit to the number of disabled SSL chips after which the ADC restarts. A value of zero implies that the ADC does not automatically restart. Default value: 0
undefactioncontrol	<String>	Read-write	Name of the undefined built-in control action: CLIENTAUTH, NOCLIENTAUTH, NOOP, RESET, or DROP.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: "CLIENTAUTH"
undefactiondata	<String>	Read-write	Name of the undefined built-in data action: NOOP, RESET or DROP. Default value: "NOOP"
defaultprofile	<String>	Read-write	Global parameter used to enable default profile feature. Default value: DISABLED Possible values = ENABLED, DISABLED
softwarecryptothreshold	<Integer>	Read-write	Citrix ADC CPU utilization threshold (in percentage) beyond which crypto operations are not done in software. A value of zero implies that CPU is not utilized for doing crypto in software. Default value: 0 Minimum value = 0 Maximum value = 100

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
hybridfipsmode	<String>	Read-write	When this mode is enabled, system will use additional crypto hardware to accelerate symmetric crypto operations. Default value: DISABLED Possible values = ENABLED, DISABLED
sigdigesttype	<String[]>	Read-write	Signature Digest Algorithms that are supported by appliance. Default value is "ALL" and it will enable the following algorithms depending on the platform. On VPX: ECDSA-SHA1 ECDSA-SHA224 ECDSA-SHA256 ECDSA-SHA384 ECDSA-SHA512 RSA-SHA1 RSA-SHA224 RSA-SHA256 RSA-SHA384 RSA-SHA512 DSA-SHA1 DSA-SHA224 DSA-SHA256 DSA-SHA384 DSA-SHA512

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			On MPX with Nitrox-III and coleto cards: RSA-SHA1 RSA-SHA224 RSA-SHA256 RSA-SHA384 RSA-SHA512 ECDSA-SHA1 ECDSA-SHA224 ECDSA-SHA256 ECDSA-SHA384 ECDSA-SHA512 Others: RSA-SHA1 RSA-SHA224 RSA-SHA256 RSA-SHA384 RSA-SHA512. Note:ALL doesnot include RSA-MD5 for any platform. Default value: ALL Possible values = ALL, RSA-MD5, RSA-SHA1, RSA-SHA224, RSA-SHA256, RSA-SHA384, RSA-SHA512, DSA-SHA1, DSA-SHA224, DSA-SHA256, DSA-SHA384, DSA-SHA512, ECDSA-

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			SHA1, ECDSA-SHA224, ECDSA-SHA256, ECDSA-SHA384, ECDSA-SHA512
sslierrorcache	<String>	Read-write	Enable or disable dynamically learning and caching the learned information to make the subsequent interception or bypass decision. When enabled, NS does the lookup of this cached data to do early bypass. Default value: DISABLED Possible values = ENABLED, DISABLED
sslimaxerrorcachemem	<Integer>	Read-write	Specify the maximum memory that can be used for caching the learned data. This memory is used as a LRU cache so that the old entries gets replaced with new entry once the set memory limit is fully utilised. A value of 0 decides the limit automatically.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: 0 Minimum value = 0 Maximum value = 4294967294
insertcertspace	<String>	Read-write	To insert space between lines in the certificate header of request. Default value: YES Possible values = YES, NO
ndcppcompliancecertcheck	<String>	Read-write	Determines whether or not additional checks are carried out during a TLS handshake when validating an X.509 certificate received from the peer. Settings apply as follows: YES - (1) During certificate verification, ignore the Common Name field (inside the subject name) if Subject Alternative Name X.509 extension is present

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			in the certificate for backend connection. (2) Verify the Extended Key Usage X.509 extension server/client leaf certificate received over the wire is consistent with the peer's role. (applicable for frontend and backend connections) (3) Verify the Basic Constraint CA field set to TRUE for non-leaf certificates. (applicable for frontend, backend connections and CAs bound to the Citrix ADC. NO - (1) Verify the Common Name

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			field (inside the subject name) irrespective of Subject Alternative Name X.509 extension. (2) Ignore the Extended Key Usage X.509 extension for server/client leaf certificate. (3) Do not verify the Basic Constraint CA true flag for non-leaf certificates. Default value: NO Possible values = YES, NO
heterogeneoussslhw	<String>	Read-write	To support both cavium and coleto based platforms in cluster environment, this mode has to be enabled. Default value: DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ENABLED, DISABLED
operationqueuelimit	<Integer>	Read-write	Limit in percentage of capacity of the crypto operations queue beyond which new SSL connections are not accepted until the queue is reduced. Default value: 150 Minimum value = 0 Maximum value = 10000
svctls1112disable	<String>	Read-only	Disable TLS 1.1 and 1.2 for dynamic and VPN created services. Default value: NO Possible values = YES, NO
montls1112disable	<String>	Read-only	Disable TLS 1.1 and 1.2 for secure (https) monitors bound to SSL_BRIDGE services. Default value: NO Possible values = YES, NO
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- UPDATE
- UNSET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslparameter **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"sslparameter":{

"quantumsize":<String_value>,

"crlmemorysizemb":<Integer_value>,

"strictcachecks":<String_value>,

"ssltriggertimeout":<Integer_value>,

"sendclosenotify":<String_value>,

"encrypttriggerpktcount":<Integer_value>,

"denysslreneg":<String_value>,

"insertionencoding":<String_value>,

"ocspcachesize":<Integer_value>,

"pushflag":<Integer_value>,

"dropreqwithnohostheader":<String_value>,

"snihttphostmatch":<String_value>,

"pushenctriggertimeout":<Integer_value>,

"cryptodevdisablelimit":<Integer_value>,

"undefactioncontrol":<String_value>,

"undefactiondata":<String_value>,

"defaultprofile":<String_value>,

"softwarecryptothreshold":<Integer_value>,

"hybridfipsmode":<String_value>,

"sigdigesttype":<String[]_value>,
```

```
"sslierrorcache":<String_value>,

"sslimaxerrorcachemem":<Integer_value>,

"insertcertspace":<String_value>,

"ndcppcompliancecertcheck":<String_value>,

"heterogeneoussslhw":<String_value>,

"operationqueuelimit":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslparameter? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"sslparameter":{

"quantumsize":true,

"crlmemorysizemb":true,

"strictcachecks":true,

"ssltriggertimeout":true,
```

```
"sendclosenotify":true,

"encrypttriggerpktcount":true,

"denysslreneg":true,

"insertionencoding":true,

"ocspcachesize":true,

"pushflag":true,

"dropreqwithnohostheader":true,

"snihttphostmatch":true,

"pushenctriggertimeout":true,

"cryptodevdisablelimit":true,

"undefactioncontrol":true,

"undefactiondata":true,

"defaultprofile":true,

"softwarecryptothreshold":true,

"hybridfipsmode":true,

"sigdigesttype":true,

"sslierrorcache":true,

"sslimaxerrorcachemem":true,

"insertcertspace":true,

"ndcppcompliancecertcheck":true,

"heterogeneoussslhw":true,

"operationqueuelimit":true
```

```
}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslparameter **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "sslparameter": [ {

"quantumsize":<String_value>,

"crlmemorysizemb":<Integer_value>,

"strictcachecks":<String_value>,

"ssltriggertimeout":<Integer_value>,

"sendclosenotify":<String_value>,

"encrypttriggerpktcount":<Integer_value>,

"denysslreneg":<String_value>,
```

```
"insertionencoding":<String_value>,

"ocspcachesize":<Integer_value>,

"pushflag":<Integer_value>,

"dropreqwithnohostheader":<String_value>,

"snihttphostmatch":<String_value>,

"pushenctriggertimeout":<Integer_value>,

"cryptodevdisablelimit":<Integer_value>,

"undefactioncontrol":<String_value>,

"undefactiondata":<String_value>,

"defaultprofile":<String_value>,

"svctls1112disable":<String_value>,

"montls1112disable":<String_value>,

"softwarecryptothreshold":<Integer_value>,

"hybridfipsmode":<String_value>,

"sigdigesttype":<String[]_value>,

"sslierrorcache":<String_value>,

"sslimaxerrorcachemem":<Integer_value>,

"insertcertspace":<String_value>,

"ndcppcompliancecertcheck":<String_value>,

"heterogeneoussslhw":<String_value>,

"operationqueuelimit":<Integer_value>,

"_nextgenapiresource":<String_value>
```

```
}]}
```

sslpkcs12

Configuration for pkcs12 resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
outfile	<String>	Read-write	Name for and, optionally, path to, the output file that contains the certificate and the private key after converting from PKCS#12 to PEM format. /nsconfig/ssl/ is the default path. If importing, the certificate-key pair is stored in PEM format. If exporting, the certificate-key pair is stored in PKCS#12 format. Maximum length = 255
Import	<Boolean>	Read-write	Convert the certificate and private-key from PKCS#12 format to PEM format.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
pkcs12file	<String>	Read-write	Name for and, optionally, path to, the PKCS#12 file. If importing, specify the input file name that contains the certificate and the private key in PKCS#12 format. If exporting, specify the output file name that contains the certificate and the private key after converting from PEM to PKCS#12 format. /nsconfig/ssl/ is the default path. During the import operation, if the key is encrypted, you are prompted to enter the pass phrase used for encrypting the key. Maximum length = 255
des	<Boolean>	Read-write	Encrypt the private key by using the DES algorithm in CBC mode during the import operation. On the command line, you are

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			prompted to enter the pass phrase.
des3	<Boolean>	Read-write	Encrypt the private key by using the Triple-DES algorithm in EDE CBC mode (168-bit key) during the import operation. On the command line, you are prompted to enter the pass phrase.
aes256	<Boolean>	Read-write	Encrypt the private key by using the AES algorithm (256-bit key) during the import operation. On the command line, you are prompted to enter the pass phrase.
export	<Boolean>	Read-write	Convert the certificate and private key from PEM format to PKCS#12 format. On the command line, you are prompted to enter the pass phrase.
certfile	<String>	Read-write	Certificate file to be converted from PEM to PKCS#12 format. Maximum length = 255

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
keyfile	<String>	Read-write	Name of the private key file to be converted from PEM to PKCS#12 format. If the key file is encrypted, you are prompted to enter the pass phrase used for encrypting the key. Maximum length = 255
password	<String>	Read-write	. Minimum length = 1 Maximum length = 31
pempassphrase	<String>	Read-write	. Minimum length = 1 Maximum length = 31

Operations

(click to see Properties)

- CONVERT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

CONVERT

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslpkcs12? **action=convert HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"sslpkcs12":{

<b>"outfile":<String_value>,

</b>"Import":<Boolean_value>,

"pkcs12file":<String_value>,

"des":<Boolean_value>,

"des3":<Boolean_value>,

"aes256":<Boolean_value>,
```

```
"export":<Boolean_value>,

"certfile":<String_value>,

"keyfile":<String_value>,

<b>"password":<String_value>,

</b>"pempassphrase":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

sslpkcs8

Configuration for pkcs8 resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
pkcs8file	<String>	Read-write	Name for and, optionally, path to, the output file where the PKCS#8 format key file is stored. /nsconfig/ssl/ is the default path. Maximum length = 255
keyfile	<String>	Read-write	Name of and, optionally, path to the input key file to be converted from PEM or DER format to

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			PKCS#8 format. /nsconfig/ssl/ is the default path. Maximum length = 255
keyform	<String>	Read-write	Format in which the key file is stored on the appliance. Default value: PEM Possible values = DER, PEM
password	<String>	Read-write	Password to assign to the file if the key is encrypted. Applies only for PEM format files. Minimum length = 1 Maximum length = 31

Operations

(click to see Properties)

- CONVERT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

CONVERT

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslpkcs8? **action=convert HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"sslpkcs8":{

<b>"pkcs8file":<String_value>,

</b><b>"keyfile":<String_value>,

</b>"keyform":<String_value>,

"password":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

sslpolicy

Configuration for SSL policy resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the new SSL policy. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the policy is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			"my policy" or 'my policy'). Minimum length = 1
rule	<String>	Read-write	Expression, against which traffic is evaluated. The following requirements apply only to the Citrix ADC CLI: * If the expression includes one or more spaces, enclose the entire expression in double quotation marks. * If the expression itself includes double quotation marks, escape the quotations by using the character. * Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
reqaction	<String>	Read-write	The name of the action to be performed on the request. Refer to 'add ssl action' command to add a new action. Builtin actions like NOOP, RESET, DROP, CLIENTAUTH and NOCLIENTAUTH are also allowed. Minimum length = 1
action	<String>	Read-write	Name of the built-in or user-defined action to perform on the request. Available built-in actions are NOOP, RESET, DROP, CLIENTAUTH, NOCLIENTAUTH, INTERCEPT AND BYPASS.
undefaction	<String>	Read-write	Name of the action to be performed when the result of rule evaluation is undefined. Possible values for control policies: CLIENTAUTH, NOCLIENTAUTH, NOOP, RESET, DROP. Possible values for data policies: NOOP,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			RESET, DROP and BYPASS.
comment	<String>	Read-write	Any comments associated with this policy.
hits	<Integer>	Read-only	Number of hits.
undefhits	<Integer>	Read-only	Number of Undef hits.
description	<String>	Read-only	Description of the policy.
builtin	<String[]>	Read-only	Flag to determine if SSL policy is built-in or not. Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL
feature	<String>	Read-only	The feature to be checked while applying this config.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET

- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslpolicy **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"sslpolicy":{

<b>"name":<String_value>,

</b><b>"rule":<String_value>,

</b>"reqaction":<String_value>,

"action":<String_value>,

"undefaction":<String_value>,

"comment":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslpolicy/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslpolicy **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"sslpolicy":{

<b>"name":<String_value>,

</b>"rule":<String_value>,

"action":<String_value>,

"undefaction":<String_value>,

"comment":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslpolicy? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"sslpolicy":{

<b>"name":<String_value>,

</b>"undefaction":true,

"comment":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslpolicy **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/sslpolicy? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/sslpolicy? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of sslpolicy resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/sslpolicy? **view=summary**

Use this query-parameter to get the summary output of sslpolicy resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/sslpolicy? **pagesize=#no;pageno=#no**

Use this query-parameter to get the sslpolicy resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "sslpolicy": [ {

"name":<String_value>,

"rule":<String_value>,

"action":<String_value>,

"undefaction":<String_value>,

"hits":<Integer_value>,

"undefhits":<Integer_value>,

"description":<String_value>,

"comment":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslpolicy/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/sslpolicy/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/sslpolicy/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of sslpolicy resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslpolicy": [ {

"name":<String_value>,

"rule":<String_value>,

"action":<String_value>,

"undefaction":<String_value>,

"hits":<Integer_value>,

"undefhits":<Integer_value>,

"description":<String_value>,

"comment":<String_value>,

"builtin":<String[]_value>,
```

```
"feature":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslpolicy? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "sslpolicy": [ { "__count": "#no"} ] }
```

sslpolicy_binding

Binding object which returns the resources bound to sslpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the SSL policy for which to

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			display detailed information. Minimum length = 1
sslpolicy_lbvserver_binding	<sslpolicy_lbvserver_binding[]>	Read-only	lbvserver that can be bound to sslpolicy.
sslpolicy_sslservice_binding	<sslpolicy_sslservice_binding[]>	Read-only	sslservice that can be bound to sslpolicy.
sslpolicy_sslvserver_binding	<sslpolicy_sslvserver_binding[]>	Read-only	sslvserver that can be bound to sslpolicy.
sslpolicy_sslglobal_binding	<sslpolicy_sslglobal_binding[]>	Read-only	sslglobal that can be bound to sslpolicy.
sslpolicy_sslpolicylabel_binding	<sslpolicy_sslpolicylabel_binding[]>	Read-only	sslpolicylabel that can be bound to sslpolicy.
sslpolicy_csvserver_binding	<sslpolicy_csvserver_binding[]>	Read-only	csvserver that can be bound to sslpolicy.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslpolicy_binding/ name_value<String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "sslpolicy_binding": [ {

"name":<String_value>,
```

```
"sslpolicy_lbvserver_binding":<sslpolicy_lbvserver_binding[]_value>,

"sslpolicy_csvserver_binding":<sslpolicy_csvserver_binding[]_value>,

"sslpolicy_sslservice_binding":<sslpolicy_sslservice_binding[]_value>,

"sslpolicy_sslpolicylabel_binding":<sslpolicy_sslpolicylabel_binding[]_val
ue>,

"sslpolicy_sslglobal_binding":<sslpolicy_sslglobal_binding[]_value>,

"sslpolicy_sslvserver_binding":<sslpolicy_sslvserver_binding[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslpolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/sslpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "sslpolicy_binding": [ {

"name":<String_value>,

"sslpolicy_lbvserver_binding":<sslpolicy_lbvserver_binding[]_value>,

"sslpolicy_csvserver_binding":<sslpolicy_csvserver_binding[]_value>,

"sslpolicy_sslservice_binding":<sslpolicy_sslservice_binding[]_value>,

"sslpolicy_sslpolicylabel_binding":<sslpolicy_sslpolicylabel_binding[]_val
ue>,

"sslpolicy_sslglobal_binding":<sslpolicy_sslglobal_binding[]_value>,

"sslpolicy_sslvserver_binding":<sslpolicy_sslvserver_binding[]_value>

}]}
```

sslpolicy_csvserver_binding

Binding object showing the csvserver that can be bound to sslpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
boundto	<String>	Read-write	The entity name to which policy is bound.
name	<String>	Read-write	Name of the SSL policy for which to display detailed information. Minimum length = 1
activepolicy	<Integer>	Read-only	.
priority	<Integer>	Read-only	.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
labeltype	<String>	Read-only	Type of policy label invocation. Possible values = vserver, service, policylabel
gotopriorityexpression	<String>	Read-only	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
labelname	<String>	Read-only	Name of the label to invoke if the current policy rule evaluates to TRUE.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslpolicy_csvserver_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ sslpolicy_csvserver_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of sslpolicy_csvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/sslpolicy_csvserver_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the sslpolicy_csvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslpolicy_csvserver_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"activepolicy":<Integer_value>,

"priority":<Integer_value>,

"labeltype":<String_value>,

"gotopriorityexpression":<String_value>,

"labelname":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslpolicy_csvserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/sslpolicy_csvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslpolicy_csvserver_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"activepolicy":<Integer_value>,

"priority":<Integer_value>,

"labeltype":<String_value>,

"gotopriorityexpression":<String_value>,

"labelname":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslpolicy_csvserver_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"sslpolicy_csvserver_binding": [ { "__count": "#no"} ] }
```

sslpolicy_lbvserver_binding

Binding object showing the lbvserver that can be bound to sslpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the SSL policy for which to display detailed information. Minimum length = 1
boundto	<String>	Read-write	The entity name to which policy is bound.
labeltype	<String>	Read-only	Type of policy label invocation. Possible values = vserver, service, policylabel
priority	<Integer>	Read-only	.
activepolicy	<Integer>	Read-only	.
labelname	<String>	Read-only	Name of the label to invoke if the current policy rule evaluates to TRUE.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
gotopriorityexpression	<String>	Read-only	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslpolicy_lbvserver_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ sslpolicy_lbvserver_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of sslpolicy_lbvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/sslpolicy_lbvserver_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the sslpolicy_lbvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslpolicy_lbvserver_binding": [ {

"name":<String_value>,

"boundto":<String_value>,
```

```
"labeltype":<String_value>,

"priority":<Integer_value>,

"activepolicy":<Integer_value>,

"labelname":<String_value>,

"gotopriorityexpression":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslpolicy_lbvserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/sslpolicy_lbvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslpolicy_lbvserver_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"activepolicy":<Integer_value>,

"labelname":<String_value>,

"gotopriorityexpression":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslpolicy_lbvserver_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"sslpolicy_lbvserver_binding": [ { "__count": "#no"} ] }
```

sslpolicy_sslglobal_binding

Binding object showing the sslglobal that can be bound to sslpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the SSL policy for which to display detailed information. Minimum length = 1
boundto	<String>	Read-write	The entity name to which policy is bound.
activepolicy	<Integer>	Read-only	.
labeltype	<String>	Read-only	Type of policy label invocation. Possible values = vserver, service, policylabel
priority	<Integer>	Read-only	.
labelname	<String>	Read-only	Name of the label to invoke if the current policy rule evaluates to TRUE.
gotopriorityexpression	<String>	Read-only	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslpolicy_sslglobal_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ sslpolicy_sslglobal_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of sslpolicy_sslglobal_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/sslpolicy_sslglobal_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the sslpolicy_sslglobal_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslpolicy_sslglobal_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"activepolicy":<Integer_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"labelname":<String_value>,

"gotopriorityexpression":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslpolicy_sslglobal_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/sslpolicy_sslglobal_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslpolicy_sslglobal_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"activepolicy":<Integer_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"labelname":<String_value>,
```

```
"gotopriorityexpression":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslpolicy_sslglobal_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"sslpolicy_sslglobal_binding": [ { "__count": "#no"} ] }
```

sslpolicy_sslpolicylabel_binding

Binding object showing the sslpolicylabel that can be bound to sslpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
boundto	<String>	Read-write	The entity name to which policy is bound.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the SSL policy for which to display detailed information. Minimum length = 1
activepolicy	<Integer>	Read-only	.
priority	<Integer>	Read-only	.
labeltype	<String>	Read-only	Type of policy label invocation. Possible values = vserver, service, policylabel
gotopriorityexpression	<String>	Read-only	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
labelname	<String>	Read-only	Name of the label to invoke if the current policy rule evaluates to TRUE.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslpolicy_sslpolicylabel_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ sslpolicy_sslpolicylabel_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of sslpolicy_sslpolicylabel_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/sslpolicy_sslpolicylabel_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the sslpolicy_sslpolicylabel_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslpolicy_sslpolicylabel_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"activepolicy":<Integer_value>,

"priority":<Integer_value>,

"labeltype":<String_value>,

"gotopriorityexpression":<String_value>,

"labelname":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslpolicy_sslpolicylabel_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/sslpolicy_sslpolicylabel_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslpolicy_sslpolicylabel_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"activepolicy":<Integer_value>,

"priority":<Integer_value>,

"labeltype":<String_value>,

"gotopriorityexpression":<String_value>,

"labelname":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslpolicy_sslpolicylabel_binding/name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"sslpolicy_sslpolicylabel_binding": [ { "__count": "#no"} ] }
```

sslpolicy_sslservice_binding

Binding object showing the sslservice that can be bound to sslpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the SSL policy for which to display detailed information. Minimum length = 1
boundto	<String>	Read-write	The entity name to which policy is bound.
gotopriorityexpression	<String>	Read-only	Expression specifying the priority of the next policy which will get evaluated if the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			current policy rule evaluates to TRUE.
labelname	<String>	Read-only	Name of the label to invoke if the current policy rule evaluates to TRUE.
priority	<Integer>	Read-only	.
labeltype	<String>	Read-only	Type of policy label invocation. Possible values = vserver, service, policylabel
activepolicy	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of

creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslpolicy_sslservice_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ sslpolicy_sslservice_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of sslpolicy_sslservice_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/sslpolicy_sslservice_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the sslpolicy_sslservice_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslpolicy_sslservice_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"gotopriorityexpression":<String_value>,

"labelname":<String_value>,

"priority":<Integer_value>,

"labeltype":<String_value>,

"activepolicy":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslpolicy_sslservice_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/sslpolicy_sslservice_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslpolicy_sslservice_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"gotopriorityexpression":<String_value>,

"labelname":<String_value>,

"priority":<Integer_value>,

"labeltype":<String_value>,

"activepolicy":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslpolicy_sslservice_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"sslpolicy_sslservice_binding": [ { "__count": "#no"} ] }
```

sslpolicy_sslvserver_binding

Binding object showing the sslvserver that can be bound to sslpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the SSL policy for which to display detailed information. Minimum length = 1
boundto	<String>	Read-write	The entity name to which policy is bound.
labeltype	<String>	Read-only	Type of policy label invocation. Possible values = vserver, service, policylabel
priority	<Integer>	Read-only	.
activepolicy	<Integer>	Read-only	.
labelname	<String>	Read-only	Name of the label to invoke if the current policy rule evaluates to TRUE.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
gotopriorityexpression	<String>	Read-only	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslpolicy_sslvserver_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ sslpolicy_sslvserver_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of sslpolicy_sslvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/sslpolicy_sslvserver_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the sslpolicy_sslvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslpolicy_sslvserver_binding": [ {

"name":<String_value>,

"boundto":<String_value>,
```

```
"labeltype":<String_value>,

"priority":<Integer_value>,

"activepolicy":<Integer_value>,

"labelname":<String_value>,

"gotopriorityexpression":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslpolicy_sslvserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/sslpolicy_sslvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslpolicy_sslvserver_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"activepolicy":<Integer_value>,

"labelname":<String_value>,

"gotopriorityexpression":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslpolicy_sslvserver_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"sslpolicy_sslvserver_binding": [ { "__count": "#no"} ] }
```

sslpolicylabel

Configuration for SSL policy label resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
labelname	<String>	Read-write	Name for the SSL policy label. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the policy label is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my label" or 'my label').

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
type	<String>	Read-write	Type of policies that the policy label can contain. Possible values = CONTROL, DATA, HTTPQUIC_CONTROL, HTTPQUIC_DATA
numpol	<Integer>	Read-only	Number of polices bound to label.
hits	<Integer>	Read-only	Number of times policy label was invoked.
policyname	<String>	Read-only	Name of the SSL policy to bind to the policy label.
priority	<Integer>	Read-only	Specifies the priority of the policy.
gotopriorityexpression	<String>	Read-only	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
invoke	<Boolean>	Read-only	Invoke flag.
labeltype	<String>	Read-only	Type of policy label invocation. Possible values = vserver, service, policylabel

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
invoke_labelname	<String>	Read-only	Name of the label to invoke if the current policy rule evaluates to TRUE.
flowtype	<Integer>	Read-only	Flowtype of the bound SSL policy.
description	<String>	Read-only	Description of the policylabel.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslpolicylabel **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"sslpolicylabel":{

<b>"labelname":<String_value>,

</b><b>"type":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslpolicylabel/ labelname_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslpolicylabel **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/sslpolicylabel? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/sslpolicylabel? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of sslpolicylabel resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/sslpolicylabel? **view=summary**

Use this query-parameter to get the summary output of sslpolicylabel resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/sslpolicylabel? **pagesize=#no;pageno=#no**

Use this query-parameter to get the sslpolicylabel resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "sslpolicylabel": [ {

"labelname":<String_value>,

"type":<String_value>,

"numpol":<Integer_value>,

"hits":<Integer_value>,

"policyname":<String_value>,

"priority":<Integer_value>,

"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>,

"labeltype":<String_value>,

"invoke_labelname":<String_value>,

"flowtype":<Integer_value>,

"description":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslpolicylabel/ labelname_value<String>
Query-parameters: attrs http:// <netscaler-ip-address> /nitro/v1/config/sslpolicylabel/ labelname_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/sslpolicylabel/ labelname_value<String> ? **view=summary**

Use this query-parameter to get the summary output of sslpolicylabel resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslpolicylabel": [ {

"labelname":<String_value>,

"type":<String_value>,

"numpol":<Integer_value>,

"hits":<Integer_value>,

"policyname":<String_value>,

"priority":<Integer_value>,

"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>,
```

```
"labeltype":<String_value>,

"invoke_labelname":<String_value>,

"flowtype":<Integer_value>,

"description":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslpolicylabel? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "sslpolicylabel": [ { "__count": "#no"} ] }
```

sslpolicylabel_binding

Binding object which returns the resources bound to sslpolicylabel.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
labelname	<String>	Read-write	Name of the SSL policy label for which to show detailed information.
sslpolicylabel_sslpolicy_binding	<sslpolicylabel_sslpolicy_binding[]>	Read-only	sslpolicy that can be bound to sslpolicylabel.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslpolicylabel_binding/ labelname_value<String>

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "sslpolicylabel_binding": [ {

"labelname":<String_value>,

"sslpolicylabel_sslpolicy_binding":<sslpolicylabel_sslpolicy_binding[]_val
ue>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslpolicylabel_binding

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters:

bulkbindings

http:// <netscaler-ip-address> /nitro/v1/config/sslpolicylabel_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "sslpolicylabel_binding": [ {

"labelname":<String_value>,

"sslpolicylabel_sslpolicy_binding":<sslpolicylabel_sslpolicy_binding[]_val
ue>

}]}
```

sslpolicylabel_sslpolicy_binding

Binding object showing the sslpolicy that can be bound to sslpolicylabel.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
invoke	<Boolean>	Read-write	Invoke policies bound to a policy label. After the invoked policies are evaluated, the flow returns to the policy with the next priority.
gotopriorityexpression	<String>	Read-write	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
policyname	<String>	Read-write	Name of the SSL policy to bind to the policy label.
invoke_labelname	<String>	Read-write	Name of the label to invoke if the current policy rule evaluates to TRUE.
labelname	<String>	Read-write	Name of the SSL policy label to which to bind policies.
priority	<Integer>	Read-write	Specifies the priority of the policy.
labeltype	<String>	Read-write	Type of policy label invocation. Possible values = vserver, service, policylabel

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/sslpolicylabel_sslpolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"sslpolicylabel_sslpolicy_binding":{

<b>"labelname":<String_value>,

</b><b>"policyname":<String_value>,

</b><b>"priority":<Integer_value>,

</b>"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>,

"labeltype":<String_value>,

"invoke_labelname":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslpolicylabel_sslpolicy_binding/ labelname_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/

sslpolicylabel_sslpolicy_binding/ labelname_value<String> ? **args= policyname:<String_value>, priority: <Integer_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslpolicylabel_sslpolicy_binding/ labelname_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ sslpolicylabel_sslpolicy_binding/ labelname_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of sslpolicylabel_sslpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/sslpolicylabel_sslpolicy_binding/ labelname_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the sslpolicylabel_sslpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslpolicylabel_sslpolicy_binding": [ {

"invoke":<Boolean_value>,

"gotopriorityexpression":<String_value>,

"policyname":<String_value>,

"invoke_labelname":<String_value>,

"labelname":<String_value>,

"priority":<Integer_value>,

"labeltype":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslpolicylabel_sslpolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/sslpolicylabel_sslpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslpolicylabel_sslpolicy_binding": [ {

"invoke":<Boolean_value>,

"gotopriorityexpression":<String_value>,

"policyname":<String_value>,

"invoke_labelname":<String_value>,

"labelname":<String_value>,

"priority":<Integer_value>,

"labeltype":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslpolicylabel_sslpolicy_binding/ labelname_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"sslpolicylabel_sslpolicy_binding": [ { "__count": "#no"} ] }
```

sslprofile

Configuration for SSL profile resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the SSL profile. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the profile is created. Minimum length = 1 Maximum length = 127
sslprofiletype	<String>	Read-write	Type of profile. Front end profiles apply to the entity that receives requests from a client. Backend profiles apply to the entity

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			that sends client requests to a server. Default value: FrontEnd Possible values = BackEnd, FrontEnd, QUIC-FrontEnd, QUIC-BackEnd
ssllogprofile	<String>	Read-write	The name of the ssllogprofile. Minimum length = 1 Maximum length = 127
dhcount	<Integer>	Read-write	Number of interactions, between the client and the Citrix ADC, after which the DH private-public pair is regenerated. A value of zero (0) specifies refresh every time. This parameter is not applicable when configuring a backend profile. Allowed DH count values are 0 and >= 500. Minimum value = 0 Maximum value = 65534

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
dh	<String>	Read-write	State of Diffie-Hellman (DH) key exchange. This parameter is not applicable when configuring a backend profile. Default value: DISABLED Possible values = ENABLED, DISABLED
dhfile	<String>	Read-write	The file name and path for the DH parameter. Minimum length = 1
ersa	<String>	Read-write	State of Ephemeral RSA (eRSA) key exchange. Ephemeral RSA allows clients that support only export ciphers to communicate with the secure server even if the server certificate does not support export clients. The ephemeral RSA key is automatically generated when you bind an export cipher to an SSL or TCP-based SSL virtual server or service.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			When you remove the export cipher, the eRSA key is not deleted. It is reused at a later date when another export cipher is bound to an SSL or TCP-based SSL virtual server or service. The eRSA key is deleted when the appliance restarts. This parameter is not applicable when configuring a backend profile. Default value: ENABLED Possible values = ENABLED, DISABLED
ersacount	<Integer>	Read-write	The refresh count for the re-generation of RSA public-key and private-key pair. Minimum value = 0 Maximum value = 65534
sessreuse	<String>	Read-write	State of session reuse. Establishing the initial handshake requires CPU-intensive public key encryption operations. With the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			ENABLED setting, session key exchange is avoided for session resumption requests received from the client. Default value: ENABLED Possible values = ENABLED, DISABLED
sesstimeout	<Integer>	Read-write	The Session timeout value in seconds. Minimum value = 0 Maximum value = 4294967294
cipherredirect	<String>	Read-write	State of Cipher Redirect. If this parameter is set to ENABLED, you can configure an SSL virtual server or service to display meaningful error messages if the SSL handshake fails because of a cipher mismatch between the virtual server or service and the client. This parameter is not applicable when

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			configuring a backend profile. Default value: DISABLED Possible values = ENABLED, DISABLED
cipherurl	<String>	Read-write	The redirect URL to be used with the Cipher Redirect feature.
clientauth	<String>	Read-write	State of client authentication. In service-based SSL offload, the service terminates the SSL handshake if the SSL client does not provide a valid certificate. This parameter is not applicable when configuring a backend profile. Default value: DISABLED Possible values = ENABLED, DISABLED
clientcert	<String>	Read-write	The rule for client certificate requirement in client authentication.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = Mandatory, Optional
dhkeyexpsizelimit	<String>	Read-write	This option enables the use of NIST recommended (NIST Special Publication 800-56A) bit size for private-key size. For example, for DH params of size 2048bit, the private-key size recommended is 224bits. This is rounded-up to 256bits. Default value: DISABLED Possible values = ENABLED, DISABLED
sslredirect	<String>	Read-write	State of HTTPS redirects for the SSL service. For an SSL session, if the client browser receives a redirect message, the browser tries to connect to the new location. However, the secure SSL session breaks if the object has moved from a secure site (https://)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			to an unsecure site (http://). Typically, a warning message appears on the screen, prompting the user to continue or disconnect. If SSL Redirect is ENABLED, the redirect message is automatically converted from http:// to https:// and the SSL session does not break. This parameter is not applicable when configuring a backend profile. Default value: DISABLED Possible values = ENABLED, DISABLED
redirectportrewrite	<String>	Read-write	State of the port rewrite while performing HTTPS redirect. If this parameter is set to ENABLED, and the URL from the server does not contain the standard port, the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			port is rewritten to the standard. Default value: DISABLED Possible values = ENABLED, DISABLED
ssl3	<String>	Read-write	State of SSLv3 protocol support for the SSL profile. Note: On platforms with SSL acceleration chips, if the SSL chip does not support SSLv3, this parameter cannot be set to ENABLED. Default value: DISABLED Possible values = ENABLED, DISABLED
tls1	<String>	Read-write	State of TLSv1.0 protocol support for the SSL profile. Default value: ENABLED Possible values = ENABLED, DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
tls11	<String>	Read-write	State of TLSv1.1 protocol support for the SSL profile. Default value: ENABLED Possible values = ENABLED, DISABLED
tls12	<String>	Read-write	State of TLSv1.2 protocol support for the SSL profile. Default value: ENABLED Possible values = ENABLED, DISABLED
tls13	<String>	Read-write	State of TLSv1.3 protocol support for the SSL profile. Default value: DISABLED Possible values = ENABLED, DISABLED
snienable	<String>	Read-write	State of the Server Name Indication (SNI) feature on the virtual server and service-based offload. SNI helps to enable SSL encryption on multiple domains on a single virtual server

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			or service if the domains are controlled by the same organization and share the same second-level domain name. For example, *.sports.net can be used to secure domains such as login.sports.net and help.sports.net. Default value: DISABLED Possible values = ENABLED, DISABLED
allowunknownsni	<String>	Read-write	Controls how the handshake is handled when the server name extension does not match any of the bound certificates. These checks are performed only if the session is SNI enabled (i.e. when profile bound to vserver has SNIEnable and Client Hello arrived with SNI extension). Available settings function as follows : ENABLED - handshakes with an unknown SNI are

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			allowed to continue, if a default cert is bound. DISLABED - handshakes with an unknown SNI are not allowed to continue. Default value: DISABLED Possible values = ENABLED, DISABLED
ocspstapling	<String>	Read-write	State of OCSP stapling support on the SSL virtual server. Supported only if the protocol used is higher than SSLv3. Possible values: ENABLED: The appliance sends a request to the OCSP responder to check the status of the server certificate and caches the response for the specified time. If the response is valid at the time of SSL handshake with the client, the OCSP-

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			based server certificate status is sent to the client during the handshake. DISABLED: The appliance does not check the status of the server certificate. . Default value: DISABLED Possible values = ENABLED, DISABLED
serverauth	<String>	Read-write	State of server authentication support for the SSL Backend profile. Default value: DISABLED Possible values = ENABLED, DISABLED
commonname	<String>	Read-write	Name to be checked against the CommonName (CN) field in the server certificate bound to the SSL server. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
pushenctrigger	<String>	Read-write	Trigger encryption on the basis of the PUSH flag value. Available settings function as follows: * ALWAYS - Any PUSH packet triggers encryption. * IGNORE - Ignore PUSH packet for triggering encryption. * MERGE - For a consecutive sequence of PUSH packets, the last PUSH packet triggers encryption. * TIMER - PUSH packet triggering encryption is delayed by the time defined in the set ssl parameter command or in the Change Advanced SSL Settings dialog box. Possible values = Always, Merge, Ignore, Timer

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
sendclosenotify	<String>	Read-write	Enable sending SSL Close-Notify at the end of a transaction. Default value: YES Possible values = YES, NO
cleartextport	<Integer>	Read-write	Port on which clear-text data is sent by the appliance to the server. Do not specify this parameter for SSL offloading with end-to-end encryption. Range 1 - 65535 * in CLI is represented as 65535 in NITRO API
insertionencoding	<String>	Read-write	Encoding method used to insert the subject or issuer's name in HTTP requests to servers. Default value: Unicode Possible values = Unicode, UTF-8
denysslreneg	<String>	Read-write	Deny renegotiation in specified circumstances. Available settings function as follows:

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			* NO - Allow SSL renegotiation. * FRONTEND_CLIENT - Deny secure and nonsecure SSL renegotiation initiated by the client. * FRONTEND_CLIENTSERVER - Deny secure and nonsecure SSL renegotiation initiated by the client or the Citrix ADC during policy-based client authentication. * ALL - Deny all secure and nonsecure SSL renegotiation. * NONSECURE - Deny nonsecure SSL renegotiation. Allows only clients that support RFC 5746. Default value: ALL

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = NO, FRONTEND_CLIENT, FRONTEND_CLIENTSERVER, ALL, NONSECURE
maxrenegrate	<Integer>	Read-write	Maximum number of renegotiation requests allowed, in one second, to each SSL entity to which this profile is bound. When set to 0, an unlimited number of renegotiation requests are allowed. Applicable only when Deny SSL renegotiation is set to a value other than ALL. Default value: 0 Minimum value = 0 Maximum value = 65535
quantumsize	<String>	Read-write	Amount of data to collect before the data is pushed to the crypto hardware for encryption. For large downloads, a larger quantum size better utilizes the crypto resources.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: 8192 Possible values = 4096, 8192, 16384
strictcachecks	<String>	Read-write	Enable strict CA certificate checks on the appliance. Default value: NO Possible values = YES, NO
encrypttriggerpktcount	<Integer>	Read-write	Maximum number of queued packets after which encryption is triggered. Use this setting for SSL transactions that send small packets from server to Citrix ADC. Default value: 45 Minimum value = 10 Maximum value = 50
pushflag	<Integer>	Read-write	Insert PUSH flag into decrypted, encrypted, or all records. If the PUSH flag is set to a value other than 0, the buffered records are forwarded on the basis of the value of the PUSH flag. Available settings function as follows:

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			0 - Auto (PUSH flag is not set.) 1 - Insert PUSH flag into every decrypted record. 2 -Insert PUSH flag into every encrypted record. 3 - Insert PUSH flag into every decrypted and encrypted record. Minimum value = 0 Maximum value = 3
dropreqwithnohostheader	<String>	Read-write	Host header check for SNI enabled sessions. If this check is enabled and the HTTP request does not contain the host header for SNI enabled sessions(i.e vserver or profile bound to vserver has SNI enabled and 'Client Hello' arrived with SNI extension), the request is dropped. Default value: NO Possible values = YES, NO

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
snihttphostmatch	<String>	Read-write	Controls how the HTTP 'Host' header value is validated. These checks are performed only if the session is SNI enabled (i.e when vserver or profile bound to vserver has SNI enabled and 'Client Hello' arrived with SNI extension) and HTTP request contains 'Host' header. Available settings function as follows: CERT - Request is forwarded if the 'Host' value is covered by the certificate used to establish this SSL session. Note: 'CERT' matching mode cannot be applied in TLS 1.3 connections established by resuming from a previous TLS 1.3 session. On these

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			connections, 'STRICT' matching mode will be used instead. STRICT - Request is forwarded only if value of 'Host' header in HTTP is identical to the 'Server name' value passed in 'Client Hello' of the SSL connection. NO - No validation is performed on the HTTP 'Host' header value. Default value: CERT Possible values = NO, CERT, STRICT
pushenctriggertimeout	<Integer>	Read-write	PUSH encryption trigger timeout value. The timeout value is applied only if you set the Push Encryption Trigger parameter to Timer in the SSL virtual server settings. Default value: 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum value = 1 Maximum value = 200
ssltriggertimeout	<Integer>	Read-write	Time, in milliseconds, after which encryption is triggered for transactions that are not tracked on the Citrix ADC because their length is not known. There can be a delay of up to 10ms from the specified timeout value before the packet is pushed into the queue. Default value: 100 Minimum value = 1 Maximum value = 200
clientauthuseboundcachain	<String>	Read-write	Certficates bound on the VIP are used for validating the client cert. Certficates came along with client cert are not used for validating the client cert. Default value: DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ENABLED, DISABLED
sslinterception	<String>	Read-write	Enable or disable transparent interception of SSL sessions. Default value: DISABLED Possible values = ENABLED, DISABLED
sslireneg	<String>	Read-write	Enable or disable triggering the client renegotiation when renegotiation request is received from the origin server. Default value: ENABLED Possible values = ENABLED, DISABLED
ssliocspcheck	<String>	Read-write	Enable or disable OCSP check for origin server certificate. Default value: ENABLED Possible values = ENABLED, DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
sslimaxsessperserver	<Integer>	Read-write	Maximum ssl session to be cached per dynamic origin server. A unique ssl session is created for each SNI received from the client on ClientHello and the matching session is used for server session reuse. Default value: 10 Minimum value = 1 Maximum value = 1000
sessionticket	<String>	Read-write	This option enables the use of session tickets, as per the RFC 5077. Default value: DISABLED Possible values = ENABLED, DISABLED
sessionticketlifetime	<Integer>	Read-write	This option sets the life time of session tickets issued by NS in secs. Default value: 300 Minimum value = 0 Maximum value = 172800

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
sessionticketkeyrefresh	<String>	Read-write	This option enables the use of session tickets, as per the RFC 5077. Default value: ENABLED Possible values = ENABLED, DISABLED
sessionticketkeydata	<String>	Read-write	Session ticket enc/dec key , admin can set it.
sessionkeylifetime	<Integer>	Read-write	This option sets the life time of symm key used to generate session tickets issued by NS in secs. Default value: 3000 Minimum value = 600 Maximum value = 86400
prevsessionkeylifetime	<Integer>	Read-write	This option sets the life time of symm key used to generate session tickets issued by NS in secs. Default value: 0 Minimum value = 0

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum value = 172800
hsts	<String>	Read-write	State of HSTS protocol support for the SSL profile. Using HSTS, a server can enforce the use of an HTTPS connection for all communication with a client. Default value: DISABLED Possible values = ENABLED, DISABLED
maxage	<Integer>	Read-write	Set the maximum time, in seconds, in the strict transport security (STS) header during which the client must send only HTTPS requests to the server. Default value: 0 Minimum value = 0 Maximum value = 4294967294
includesubdomains	<String>	Read-write	Enable HSTS for subdomains. If set to Yes, a client must send only HTTPS

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			requests for subdomains. Default value: NO Possible values = YES, NO
preload	<String>	Read-write	Flag indicates the consent of the site owner to have their domain preloaded. Default value: NO Possible values = YES, NO
skipclientcertpolicycheck	<String>	Read-write	This flag controls the processing of X509 certificate policies. If this option is Enabled, then the policy check in Client authentication will be skipped. This option can be used only when Client Authentication is Enabled and ClientCert is set to Mandatory. Default value: DISABLED Possible values = ENABLED, DISABLED
zerorttearlydata	<String>	Read-write	State of TLS 1.3 0-RTT early data support for the SSL Virtual Server. This

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			setting only has an effect if resumption is enabled, as early data cannot be sent along with an initial handshake. Early application data has significantly different security properties - in particular there is no guarantee that the data cannot be replayed. Default value: DISABLED Possible values = ENABLED, DISABLED
tls13sessionticketsperauthcontext	<Integer>	Read-write	Number of tickets the SSL Virtual Server will issue anytime TLS 1.3 is negotiated, ticket-based resumption is enabled, and either (1) a handshake completes or (2) post-handhsake client auth completes. This value can be increased to enable clients to open multiple parallel

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			connections using a fresh ticket for each connection. No tickets are sent if resumption is disabled. Default value: 1 Minimum value = 1 Maximum value = 10
dhekeyexchangewithpsk	<String>	Read-write	Whether or not the SSL Virtual Server will require a DHE key exchange to occur when a PSK is accepted during a TLS 1.3 resumption handshake. A DHE key exchange ensures forward secrecy even in the event that ticket keys are compromised, at the expense of an additional round trip and resources required to carry out the DHE key exchange. If disabled, a DHE key exchange will be performed when

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			a PSK is accepted but only if requested by the client. If enabled, the server will require a DHE key exchange when a PSK is accepted regardless of whether the client supports combined PSK-DHE key exchange. This setting only has an effect when resumption is enabled. Default value: NO Possible values = YES, NO
allowextendedmaster secret	<String>	Read-write	When set to YES, attempt to use the TLS Extended Master Secret (EMS, as described in RFC 7627) when negotiating TLS 1.0, TLS 1.1 and TLS 1.2 connection parameters. EMS must be supported

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			by both the TLS client and server in order to be enabled during a handshake. This setting applies to both frontend and backend SSL profiles. Default value: NO Possible values = YES, NO
allowlegacykdf	<String>	Read-write	FIPS 140-3 certification requires all handshakes without EMS be blocked. Such KDFs are allowed by default. This setting is to allow/disallow such legacy KDFs when needed. This setting applies to both frontend and backend SSL profiles. Default value: YES Possible values = YES, NO

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
alpnprotocol	<String>	Read-write	Application protocol supported by the server and used in negotiation of the protocol with the client. Possible values are HTTP1.1, HTTP2 and NONE. Default value is NONE which implies application protocol is not enabled hence remain unknown to the TLS layer. This parameter is relevant only if SSL connection is handled by the virtual server of the type SSL_TCP. Default value: NONE Possible values = NONE, HTTP1.1, HTTP2
encryptedclienthello	<String>	Read-write	State of TLS 1.3 Encrypted Client Hello Support. Default value: DISABLED Possible values = ENABLED, DISABLED
defaultsni	<String>	Read-write	Default domain name supported by the SSL virtual

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			server. The parameter is effective, when zero touch certificate management is active for the SSL virtual server i.e. no manual SNI cert or default server cert is bound to the v-server. For SSL transactions, when SNI is not presented by the client, server-certificate corresponding to the default SNI, if available in the cert-store, is selected else connection is terminated. Minimum length = 1 Maximum length = 126
sslclientlogs	<String>	Read-write	When enabled, NetScaler will log the session ID and SNI name during SSL handshakes on both the external and internal interfaces. Default value: DISABLED Possible values = ENABLED, DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
strictclientekucheck	<String>	Read-write	Enable strict EKU extension check during client authentication. Default value: ENABLED Possible values = ENABLED, DISABLED
dynamicclientcert	<String>	Read-write	Enable or disable Dynamic Client Certificate Generation for SSL sessions. Default value: DISABLED Possible values = ENABLED, DISABLED
ciphername	<String>	Read-write	The cipher group/ alias/individual cipher configuration.
cipherpriority	<Integer>	Read-write	cipher priority. Minimum value = 1
strictsigdigestcheck	<String>	Read-write	Parameter indicating to check whether peer entity certificate during TLS1.2 handshake is signed with one of signature-hash combination supported by Citrix ADC.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: DISABLED Possible values = ENABLED, DISABLED
nonfipsciphers	<String>	Read-only	State of usage of ciphers that are not FIPS approved. Valid only for an SSL service bound with a FIPS key and certificate. Default value: DISABLED Possible values = ENABLED, DISABLED
crlcheck	<String>	Read-only	The state of the CRL check parameter. (Mandatory/ Optional). Possible values = Mandatory, Optional
ocspcheck	<String>	Read-only	The state of the OCSP check parameter. (Mandatory/ Optional). Possible values = Mandatory, Optional
snicert	<Boolean>	Read-only	The name of the CertKey. Use this option to bind Certkey(s) which will

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			be used in SNI processing.
skipcaname	<Boolean>	Read-only	The flag is used to indicate whether this particular CA certificate's CA_Name needs to be sent to the SSL client while requesting for client certificate in a SSL handshake.
invoke	<Boolean>	Read-only	Invoke flag. This attribute is relevant only for ADVANCED policies.
labeltype	<String>	Read-only	Type of policy label invocation. Possible values = vserver, service, policylabel
service	<Integer>	Read-only	Service.
builtin	<String[]>	Read-only	Flag to determine whether ssl profile is built-in or not. Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
feature	<String>	Read-only	The feature to be checked while applying this config.
sslpfobjecttype	<Integer>	Read-only	Internal flag to indicate what type of object binds this profile: monitor or service.
ssliverifyservercertforreuse	<String>	Read-only	Verify the origin server's certificate before reusing the front-end SSL session. Making it hidden since we always verify for now. Default value: ENABLED Possible values = ENABLED, DISABLED
nodefaultbindings	<String>	Read-only	When set to YES, the SSL profile will not have default Cipher and Elliptic Curve bindings. Default value: NO Possible values = YES, NO
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslprofile **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"sslprofile":{

<b>"name":<String_value>,

</b>"sslprofiletype":<String_value>,

"ssllogprofile":<String_value>,

"dhcount":<Integer_value>,

"dh":<String_value>,

"dhfile":<String_value>,

"ersa":<String_value>,

"ersacount":<Integer_value>,

"sessreuse":<String_value>,

"sesstimeout":<Integer_value>,

"cipherredirect":<String_value>,

"cipherurl":<String_value>,

"clientauth":<String_value>,

"clientcert":<String_value>,

"dhkeyexpsizelimit":<String_value>,

"sslredirect":<String_value>,

"redirectportrewrite":<String_value>,
```

```
"ssl3":<String_value>,

"tls1":<String_value>,

"tls11":<String_value>,

"tls12":<String_value>,

"tls13":<String_value>,

"snienable":<String_value>,

"allowunknownsni":<String_value>,

"ocspstapling":<String_value>,

"serverauth":<String_value>,

"commonname":<String_value>,

"pushenctrigger":<String_value>,

"sendclosenotify":<String_value>,

"cleartextport":<Integer_value>,

"insertionencoding":<String_value>,

"denysslreneg":<String_value>,

"maxrenegrate":<Integer_value>,

"quantumsize":<String_value>,

"strictcachecks":<String_value>,

"encrypttriggerpktcount":<Integer_value>,

"pushflag":<Integer_value>,

"dropreqwithnohostheader":<String_value>,

"snihttphostmatch":<String_value>,
```

```
"pushenctriggertimeout":<Integer_value>,

"ssltriggertimeout":<Integer_value>,

"clientauthuseboundcachain":<String_value>,

"sslinterception":<String_value>,

"sslireneg":<String_value>,

"ssliocspcheck":<String_value>,

"sslimaxsessperserver":<Integer_value>,

"sessionticket":<String_value>,

"sessionticketlifetime":<Integer_value>,

"sessionticketkeyrefresh":<String_value>,

"sessionticketkeydata":<String_value>,

"sessionkeylifetime":<Integer_value>,

"prevsessionkeylifetime":<Integer_value>,

"hsts":<String_value>,

"maxage":<Integer_value>,

"includesubdomains":<String_value>,

"preload":<String_value>,

"skipclientcertpolicycheck":<String_value>,

"zerorttearlydata":<String_value>,

"tls13sessionticketsperauthcontext":<Integer_value>,

"dhekeyexchangewithpsk":<String_value>,

"allowextendedmastersecret":<String_value>,
```

```
"allowlegacykdf":<String_value>,

"alpnprotocol":<String_value>,

"encryptedclienthello":<String_value>,

"defaultsni":<String_value>,

"sslclientlogs":<String_value>,

"strictclientekucheck":<String_value>,

"dynamicclientcert":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslprofile/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslprofile **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"sslprofile":{

<b>"name":<String_value>,

</b>"ssllogprofile":<String_value>,

"dh":<String_value>,

"dhfile":<String_value>,

"dhcount":<Integer_value>,

"dhkeyexpsizelimit":<String_value>,

"ersa":<String_value>,

"ersacount":<Integer_value>,

"sessreuse":<String_value>,

"sesstimeout":<Integer_value>,

"cipherredirect":<String_value>,

"cipherurl":<String_value>,

"clientauth":<String_value>,

"clientcert":<String_value>,

"sslredirect":<String_value>,

"redirectportrewrite":<String_value>,

"ssl3":<String_value>,

"tls1":<String_value>,

"tls11":<String_value>,

"tls12":<String_value>,
```

```
"tls13":<String_value>,

"snienable":<String_value>,

"allowunknownsni":<String_value>,

"ocspstapling":<String_value>,

"serverauth":<String_value>,

"commonname":<String_value>,

"pushenctrigger":<String_value>,

"sendclosenotify":<String_value>,

"cleartextport":<Integer_value>,

"insertionencoding":<String_value>,

"denysslreneg":<String_value>,

"maxrenegrate":<Integer_value>,

"quantumsize":<String_value>,

"strictcachecks":<String_value>,

"encrypttriggerpktcount":<Integer_value>,

"pushflag":<Integer_value>,

"dropreqwithnohostheader":<String_value>,

"snihttphostmatch":<String_value>,

"pushenctriggertimeout":<Integer_value>,

"ssltriggertimeout":<Integer_value>,

"clientauthuseboundcachain":<String_value>,

"sslinterception":<String_value>,
```

```
"sslireneg":<String_value>,

"ssliocspcheck":<String_value>,

"sslimaxsessperserver":<Integer_value>,

"hsts":<String_value>,

"maxage":<Integer_value>,

"includesubdomains":<String_value>,

"preload":<String_value>,

"sessionticket":<String_value>,

"sessionticketlifetime":<Integer_value>,

"sessionticketkeyrefresh":<String_value>,

"sessionticketkeydata":<String_value>,

"sessionkeylifetime":<Integer_value>,

"prevsessionkeylifetime":<Integer_value>,

"ciphername":<String_value>,

"cipherpriority":<Integer_value>,

"strictsigdigestcheck":<String_value>,

"skipclientcertpolicycheck":<String_value>,

"zerorttearlydata":<String_value>,

"tls13sessionticketsperauthcontext":<Integer_value>,

"dhekeyexchangewithpsk":<String_value>,

"allowextendedmastersecret":<String_value>,

"allowlegacykdf":<String_value>,
```

```
"alpnprotocol":<String_value>,

"encryptedclienthello":<String_value>,

"defaultsni":<String_value>,

"sslclientlogs":<String_value>,

"strictclientekucheck":<String_value>,

"dynamicclientcert":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslprofile? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"sslprofile":{

<b>"name":<String_value>,

</b>"ssllogprofile":true,

"dh":true,

"dhfile":true,

"dhcount":true,
```

```
"dhkeyexpsizelimit":true,

"ersa":true,

"ersacount":true,

"sessreuse":true,

"sesstimeout":true,

"cipherredirect":true,

"cipherurl":true,

"clientauth":true,

"clientcert":true,

"sslredirect":true,

"redirectportrewrite":true,

"ssl3":true,

"tls1":true,

"tls11":true,

"tls12":true,

"tls13":true,

"snienable":true,

"allowunknownsni":true,

"ocspstapling":true,

"serverauth":true,

"commonname":true,

"pushenctrigger":true,
```

```
"sendclosenotify":true,

"cleartextport":true,

"insertionencoding":true,

"denysslreneg":true,

"maxrenegrate":true,

"quantumsize":true,

"strictcachecks":true,

"encrypttriggerpktcount":true,

"pushflag":true,

"dropreqwithnohostheader":true,

"snihttphostmatch":true,

"pushenctriggertimeout":true,

"ssltriggertimeout":true,

"clientauthuseboundcachain":true,

"sslinterception":true,

"sslireneg":true,

"ssliocspcheck":true,

"sslimaxsessperserver":true,

"hsts":true,

"maxage":true,

"includesubdomains":true,

"preload":true,
```

```
"sessionticket":true,

"sessionticketlifetime":true,

"sessionticketkeyrefresh":true,

"sessionticketkeydata":true,

"sessionkeylifetime":true,

"prevsessionkeylifetime":true,

"ciphername":true,

"cipherpriority":true,

"strictsigdigestcheck":true,

"skipclientcertpolicycheck":true,

"zerorttearlydata":true,

"tls13sessionticketsperauthcontext":true,

"dhekeyexchangewithpsk":true,

"allowextendedmastersecret":true,

"allowlegacykdf":true,

"alpnprotocol":true,

"encryptedclienthello":true,

"defaultsni":true,

"sslclientlogs":true,

"strictclientekucheck":true,

"dynamicclientcert":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslprofile **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/sslprofile? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/sslprofile? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of sslprofile resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/sslprofile? **view=summary**

Use this query-parameter to get the summary output of sslprofile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/sslprofile? **pagesize=#no;pageno=#no**

Use this query-parameter to get the sslprofile resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "sslprofile": [ {

"name":<String_value>,

"dh":<String_value>,

"dhfile":<String_value>,

"dhcount":<Integer_value>,

"dhkeyexpsizelimit":<String_value>,

"ersa":<String_value>,

"ersacount":<Integer_value>,

"sessreuse":<String_value>,

"sesstimeout":<Integer_value>,

"cipherredirect":<String_value>,

"cipherurl":<String_value>,

"clientauth":<String_value>,

"clientcert":<String_value>,

"sslredirect":<String_value>,

"redirectportrewrite":<String_value>,

"nonfipsciphers":<String_value>,

"ssl3":<String_value>,

"tls1":<String_value>,

"tls11":<String_value>,
```

```
"tls12":<String_value>,

"tls13":<String_value>,

"snienable":<String_value>,

"allowunknownsni":<String_value>,

"ocspstapling":<String_value>,

"serverauth":<String_value>,

"commonname":<String_value>,

"pushenctrigger":<String_value>,

"sendclosenotify":<String_value>,

"cleartextport":<Integer_value>,

"insertionencoding":<String_value>,

"denysslreneg":<String_value>,

"maxrenegrate":<Integer_value>,

"quantumsize":<String_value>,

"strictcachecks":<String_value>,

"encrypttriggerpktcount":<Integer_value>,

"pushflag":<Integer_value>,

"dropreqwithnohostheader":<String_value>,

"snihttphostmatch":<String_value>,

"pushenctriggertimeout":<Integer_value>,

"ssltriggertimeout":<Integer_value>,

"cipherpriority":<Integer_value>,
```

```
"ciphername":<String_value>,

"crlcheck":<String_value>,

"ocspcheck":<String_value>,

"snicert":<Boolean_value>,

"skipcaname":<Boolean_value>,

"invoke":<Boolean_value>,

"labeltype":<String_value>,

"sslprofiletype":<String_value>,

"clientauthuseboundcachain":<String_value>,

"ssllogprofile":<String_value>,

"service":<Integer_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"sslpfobjecttype":<Integer_value>,

"sslinterception":<String_value>,

"ssliverifyservercertforreuse":<String_value>,

"sslireneg":<String_value>,

"ssliocspcheck":<String_value>,

"sslimaxsessperserver":<Integer_value>,

"sessionticket":<String_value>,

"sessionticketlifetime":<Integer_value>,

"sessionticketkeyrefresh":<String_value>,
```

```
"sessionticketkeydata":<String_value>,

"sessionkeylifetime":<Integer_value>,

"prevsessionkeylifetime":<Integer_value>,

"hsts":<String_value>,

"maxage":<Integer_value>,

"includesubdomains":<String_value>,

"preload":<String_value>,

"strictsigdigestcheck":<String_value>,

"skipclientcertpolicycheck":<String_value>,

"zerorttearlydata":<String_value>,

"tls13sessionticketsperauthcontext":<Integer_value>,

"dhekeyexchangewithpsk":<String_value>,

"allowextendedmastersecret":<String_value>,

"allowlegacykdf":<String_value>,

"alpnprotocol":<String_value>,

"nodefaultbindings":<String_value>,

"encryptedclienthello":<String_value>,

"defaultsni":<String_value>,

"sslclientlogs":<String_value>,

"strictclientekucheck":<String_value>,

"dynamicclientcert":<String_value>,

"_nextgenapiresource":<String_value>
```

```
}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslprofile/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/sslprofile/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/sslprofile/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of sslprofile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslprofile": [ {

"name":<String_value>,

"dh":<String_value>,
```

```
"dhfile":<String_value>,

"dhcount":<Integer_value>,

"dhkeyexpsizelimit":<String_value>,

"ersa":<String_value>,

"ersacount":<Integer_value>,

"sessreuse":<String_value>,

"sesstimeout":<Integer_value>,

"cipherredirect":<String_value>,

"cipherurl":<String_value>,

"clientauth":<String_value>,

"clientcert":<String_value>,

"sslredirect":<String_value>,

"redirectportrewrite":<String_value>,

"nonfipsciphers":<String_value>,

"ssl3":<String_value>,

"tls1":<String_value>,

"tls11":<String_value>,

"tls12":<String_value>,

"tls13":<String_value>,

"snienable":<String_value>,

"allowunknownsni":<String_value>,

"ocspstapling":<String_value>,
```

```
"serverauth":<String_value>,

"commonname":<String_value>,

"pushenctrigger":<String_value>,

"sendclosenotify":<String_value>,

"cleartextport":<Integer_value>,

"insertionencoding":<String_value>,

"denysslreneg":<String_value>,

"maxrenegrate":<Integer_value>,

"quantumsize":<String_value>,

"strictcachecks":<String_value>,

"encrypttriggerpktcount":<Integer_value>,

"pushflag":<Integer_value>,

"dropreqwithnohostheader":<String_value>,

"snihttphostmatch":<String_value>,

"pushenctriggertimeout":<Integer_value>,

"ssltriggertimeout":<Integer_value>,

"cipherpriority":<Integer_value>,

"ciphername":<String_value>,

"crlcheck":<String_value>,

"ocspcheck":<String_value>,

"snicert":<Boolean_value>,

"skipcaname":<Boolean_value>,
```

```
"invoke":<Boolean_value>,

"labeltype":<String_value>,

"sslprofiletype":<String_value>,

"clientauthuseboundcachain":<String_value>,

"ssllogprofile":<String_value>,

"service":<Integer_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"sslpfobjecttype":<Integer_value>,

"sslinterception":<String_value>,

"ssliverifyservercertforreuse":<String_value>,

"sslireneg":<String_value>,

"ssliocspcheck":<String_value>,

"sslimaxsessperserver":<Integer_value>,

"sessionticket":<String_value>,

"sessionticketlifetime":<Integer_value>,

"sessionticketkeyrefresh":<String_value>,

"sessionticketkeydata":<String_value>,

"sessionkeylifetime":<Integer_value>,

"prevsessionkeylifetime":<Integer_value>,

"hsts":<String_value>,

"maxage":<Integer_value>,
```

```
"includesubdomains":<String_value>,

"preload":<String_value>,

"strictsigdigestcheck":<String_value>,

"skipclientcertpolicycheck":<String_value>,

"zerorttearlydata":<String_value>,

"tls13sessionticketsperauthcontext":<Integer_value>,

"dhekeyexchangewithpsk":<String_value>,

"allowextendedmastersecret":<String_value>,

"allowlegacykdf":<String_value>,

"alpnprotocol":<String_value>,

"nodefaultbindings":<String_value>,

"encryptedclienthello":<String_value>,

"defaultsni":<String_value>,

"sslclientlogs":<String_value>,

"strictclientekucheck":<String_value>,

"dynamicclientcert":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslprofile? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "sslprofile": [ { "__count": "#no"} ] }
```

sslprofile_binding

Binding object which returns the resources bound to sslprofile.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the SSL profile for which to show detailed information. Minimum length = 1 Maximum length = 127
sslprofile_sslvserver_binding	<sslprofile_sslvserver_binding[]>	Read-only	sslvserver that can be bound to sslprofile.
sslprofile_sslechconfig_binding	<sslprofile_sslechconfig_binding[]>	Read-only	sslechconfig that can be bound to sslprofile.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
sslprofile_sslcipher_binding	<sslprofile_sslcipher_binding[]>	Read-only	sslcipher that can be bound to sslprofile.
sslprofile_sslcertkey_binding	<sslprofile_sslcertkey_binding[]>	Read-only	sslcertkey that can be bound to sslprofile.
sslprofile_ecccurve_binding	<sslprofile_ecccurve_binding[]>	Read-only	ecccurve that can be bound to sslprofile.
sslprofile_sslciphersuite_binding	<sslprofile_sslciphersuite_binding[]>	Read-only	sslciphersuite that can be bound to sslprofile.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslprofile_binding/ name_value<String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "sslprofile_binding": [ {

"name":<String_value>,

"sslprofile_sslciphersuite_binding":<sslprofile_sslciphersuite_binding[]_value>,

"sslprofile_sslechconfig_binding":<sslprofile_sslechconfig_binding[]_value>,

"sslprofile_sslcipher_binding":<sslprofile_sslcipher_binding[]_value>,

"sslprofile_ecccurve_binding":<sslprofile_ecccurve_binding[]_value>,

"sslprofile_sslcertkey_binding":<sslprofile_sslcertkey_binding[]_value>,
```

```
"sslprofile_sslvserver_binding":<sslprofile_sslvserver_binding[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslprofile_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/sslprofile_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "sslprofile_binding": [ {

"name":<String_value>,

"sslprofile_sslciphersuite_binding":<sslprofile_sslciphersuite_binding[]_value>,

"sslprofile_sslechconfig_binding":<sslprofile_sslechconfig_binding[]_value>,

"sslprofile_sslcipher_binding":<sslprofile_sslcipher_binding[]_value>,
```

```
"sslprofile_ecccurve_binding":<sslprofile_ecccurve_binding[]_value>,

"sslprofile_sslcertkey_binding":<sslprofile_sslcertkey_binding[]_value>,

"sslprofile_sslvserver_binding":<sslprofile_sslvserver_binding[]_value>

}]}
```

sslprofile_ecccurve_binding

Binding object showing the ecccurve that can be bound to sslprofile.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ecccurvename	<String>	Read-write	Named ECC curve bound to vserver/ service. Possible values = ALL, P_224, P_256, P_384, P_521, X_25519, X25519_MLKEM768
cipherpriority	<Integer>	Read-write	Priority of the cipher binding. Minimum value = 1 Maximum value = 1000
name	<String>	Read-write	Name of the SSL profile. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum length = 127
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/sslprofile_ecccurve_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"sslprofile_ecccurve_binding":{

<b>"name":<String_value>,

</b>"cipherpriority":<Integer_value>,

"ecccurvename":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslprofile_ecccurve_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ sslprofile_ecccurve_binding/ name_value<String> ? **args=ecccurvename: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslprofile_ecccurve_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ sslprofile_ecccurve_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of sslprofile_ecccurve_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/sslprofile_ecccurve_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the sslprofile_ecccurve_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslprofile_ecccurve_binding": [ {

"ecccurvename":<String_value>,

"cipherpriority":<Integer_value>,

"name":<String_value>
```

```
}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslprofile_ecccurve_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/sslprofile_ecccurve_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslprofile_ecccurve_binding": [ {

"ecccurvename":<String_value>,

"cipherpriority":<Integer_value>,

"name":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslprofile_ecccurve_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"sslprofile_ecccurve_binding": [ { "__count": "#no"} ] }
```

sslprofile_forgingcacertkey_binding

Binding object showing the forgingcacertkey that can be bound to sslprofile.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the SSL profile. Minimum length = 1 Maximum length = 127
cipherpriority	<Integer>	Read-write	Priority of the cipher binding.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum value = 1 Maximum value = 1000
forgingcacertkey	<String>	Read-write	The certkey (CA certificate + private key) to be used for signing Forged Client Certificate.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/sslprofile_forgingcacertkey_binding

HTTP Method: PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"sslprofile_forgingcacertkey_binding":{

<b>"name":<String_value>,

</b>"cipherpriority":<Integer_value>,

"forgingcacertkey":<String_value>

}}
```

Response:

HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslprofile_forgingcacertkey_binding/ name_value<String>

Query-parameters:

args

http:// <netscaler-ip-address> /nitro/v1/config/sslprofile_forgingcacertkey_binding/ name_value<String> ? **args=forgingcacertkey: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslprofile_forgingcacertkey_binding/ name_value<String>

Query-parameters:

filter

http:// <netscaler-ip-address> /nitro/v1/config/sslprofile_forgingcacertkey_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of sslprofile_forgingcacertkey_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination

http:// <netscaler-ip-address> /nitro/v1/config/sslprofile_forgingcacertkey_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the sslprofile_forgingcacertkey_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslprofile_forgingcacertkey_binding": [ {

"name":<String_value>,

"cipherpriority":<Integer_value>,

"forgingcacertkey":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslprofile_forgingcacertkey_binding

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters:

bulkbindings

http:// <netscaler-ip-address> /nitro/v1/config/sslprofile_forgingcacertkey_binding?**bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslprofile_forgingcacertkey_binding": [ {

"name":<String_value>,

"cipherpriority":<Integer_value>,

"forgingcacertkey":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslprofile_forgingcacertkey_binding/ name_value<String> ? **count=yes**

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"sslprofile_forgingcacertkey_binding": [ { "__count": "#no"} ] }
```

sslprofile_sslcertkey_binding

Binding object showing the sslcertkey that can be bound to sslprofile.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the SSL profile. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum length = 127
cipherpriority	<Integer>	Read-write	Priority of the cipher binding. Minimum value = 1 Maximum value = 1000
forgingcacertkey	<Boolean>	Read-write	The certkey (CA certificate + private key) to be used for signing Forged Client Certificate.
certkeyname	<String>	Read-write	The certkey (CA certificate + private key) to be bound with profile.
sslicacertkey	<String>	Read-write	The certkey (CA certificate + private key) to be used for SSL interception.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/sslprofile_sslcertkey_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"sslprofile_sslcertkey_binding":{

<b>"name":<String_value>,
```

```
</b>"cipherpriority":<Integer_value>,

"certkeyname":<String_value>,

"forgingcacertkey":<Boolean_value>,

"sslicacertkey":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslprofile_sslcertkey_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ sslprofile_sslcertkey_binding/ name_value<String> ? **args=certkeyname: <String_value> ,forgingcacertkey: <Boolean_value> ,sslicacertkey: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslprofile_sslcertkey_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ sslprofile_sslcertkey_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of sslprofile_sslcertkey_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/sslprofile_sslcertkey_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the sslprofile_sslcertkey_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslprofile_sslcertkey_binding": [ {

"name":<String_value>,

"cipherpriority":<Integer_value>,

"forgingcacertkey":<Boolean_value>,

"certkeyname":<String_value>,

"sslicacertkey":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslprofile_sslcertkey_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/sslprofile_sslcertkey_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslprofile_sslcertkey_binding": [ {

"name":<String_value>,

"cipherpriority":<Integer_value>,

"forgingcacertkey":<Boolean_value>,

"certkeyname":<String_value>,

"sslicacertkey":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslprofile_sslcertkey_binding/name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"sslprofile_sslcertkey_binding": [ { "__count": "#no"} ] }
```

sslprofile_sslcipher_binding

Binding object showing the sslcipher that can be bound to sslprofile.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ciphername	<String>	Read-write	Name of the cipher. Minimum length = 1
description	<String>	Read-write	The cipher suite description.
cipheraliasname	<String>	Read-write	The name of the cipher group/alias/ individual cipheri bindings.
name	<String>	Read-write	Name of the SSL profile. Minimum length = 1 Maximum length = 127

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
cipherpriority	<Integer>	Read-write	cipher priority. Minimum value = 1
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/sslprofile_sslcipher_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"sslprofile_sslcipher_binding":{

<b>"name":<String_value>,

</b>"ciphername":<String_value>,

"cipherpriority":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslprofile_sslcipher_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ sslprofile_sslcipher_binding/ name_value<String> ? **args=ciphername: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslprofile_sslcipher_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ sslprofile_sslcipher_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of sslprofile_sslcipher_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/sslprofile_sslcipher_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the sslprofile_sslcipher_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslprofile_sslcipher_binding": [ {

"ciphername":<String_value>,

"description":<String_value>,

"cipheraliasname":<String_value>,
```

```
"name":<String_value>,

"cipherpriority":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslprofile_sslcipher_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/sslprofile_sslcipher_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslprofile_sslcipher_binding": [ {

"ciphername":<String_value>,

"description":<String_value>,

"cipheraliasname":<String_value>,
```

```
"name":<String_value>,

"cipherpriority":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslprofile_sslcipher_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"sslprofile_sslcipher_binding": [ { "__count": "#no"} ] }
```

sslprofile_sslciphersuite_binding

Binding object showing the sslciphersuite that can be bound to sslprofile.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
cipherpriority	<Integer>	Read-write	cipher priority. Minimum value = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the SSL profile. Minimum length = 1 Maximum length = 127
description	<String>	Read-write	The cipher suite description.
ciphername	<String>	Read-write	The cipher group/ alias/individual cipher configuration.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.
- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of

creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/sslprofile_sslciphersuite_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"sslprofile_sslciphersuite_binding":{

<b>"name":<String_value>,

</b>"ciphername":<String_value>,

"cipherpriority":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslprofile_sslciphersuite_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ sslprofile_sslciphersuite_binding/ name_value<String> ? **args=ciphername: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslprofile_sslciphersuite_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ sslprofile_sslciphersuite_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of sslprofile_sslciphersuite_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/sslprofile_sslciphersuite_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the sslprofile_sslciphersuite_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslprofile_sslciphersuite_binding": [ {

"cipherpriority":<Integer_value>,

"name":<String_value>,

"description":<String_value>,

"ciphername":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslprofile_sslciphersuite_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/sslprofile_sslciphersuite_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslprofile_sslciphersuite_binding": [ {

"cipherpriority":<Integer_value>,

"name":<String_value>,

"description":<String_value>,

"ciphername":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslprofile_sslciphersuite_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"sslprofile_sslciphersuite_binding": [ { "__count": "#no"} ] }
```

sslprofile_sslechconfig_binding

Binding object showing the sslechconfig that can be bound to sslprofile.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
cipherpriority	<Integer>	Read-write	Priority of the cipher binding. Minimum value = 1 Maximum value = 1000
name	<String>	Read-write	Name of the SSL profile. Minimum length = 1 Maximum length = 127
echconfigname	<String>	Read-write	Configuration for the Encrypted Client Hello feature.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/sslprofile_sslechconfig_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"sslprofile_sslechconfig_binding":{

<b>"name":<String_value>,
```

```
</b>"cipherpriority":<Integer_value>,

"echconfigname":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslprofile_sslechconfig_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ sslprofile_sslechconfig_binding/ name_value<String> ? **args=echconfigname: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslprofile_sslechconfig_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ sslprofile_sslechconfig_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of sslprofile_sslechconfig_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/sslprofile_sslechconfig_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the sslprofile_sslechconfig_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslprofile_sslechconfig_binding": [ {

"cipherpriority":<Integer_value>,

"name":<String_value>,

"echconfigname":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslprofile_sslechconfig_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/sslprofile_sslechconfig_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslprofile_sslechconfig_binding": [ {

"cipherpriority":<Integer_value>,

"name":<String_value>,

"echconfigname":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslprofile_sslechconfig_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"sslprofile_sslechconfig_binding": [ { "__count": "#no"} ] }
```

sslprofile_sslvserver_binding

Binding object showing the sslvserver that can be bound to sslprofile.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
description	<String>	Read-write	The cipher suite description.
servicename	<String>	Read-write	Service name.
cipherpriority	<Integer>	Read-write	Priority of the cipher binding. Minimum value = 1 Maximum value = 1000
name	<String>	Read-write	Name of the SSL profile. Minimum length = 1 Maximum length = 127
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslprofile_sslvserver_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ sslprofile_sslvserver_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of sslprofile_sslvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/sslprofile_sslvserver_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the sslprofile_sslvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslprofile_sslvserver_binding": [ {

"description":<String_value>,

"servicename":<String_value>,

"cipherpriority":<Integer_value>,

"name":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslprofile_sslvserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/sslprofile_sslvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslprofile_sslvserver_binding": [ {

"description":<String_value>,

"servicename":<String_value>,

"cipherpriority":<Integer_value>,

"name":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslprofile_sslvserver_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"sslprofile_sslvserver_binding": [ { "__count": "#no"} ] }
```

sslrsakey

Configuration for RSA key resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
keyfile	<String>	Read-write	Name for and, optionally, path to the RSA key file. /nsconfig/ssl/ is the default path. Maximum length = 63
bits	<Integer>	Read-write	Size, in bits, of the RSA key. Minimum value = 512 Maximum value = 4096
exponent	<String>	Read-write	Public exponent for the RSA key. The exponent is part of the cipher algorithm and is required for creating the RSA key. Default value: F4 Possible values = 3, F4

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
keyform	<String>	Read-write	Format in which the RSA key file is stored on the appliance. Default value: PEM Possible values = DER, PEM
des	<Boolean>	Read-write	Encrypt the generated RSA key by using the DES algorithm. On the command line, you are prompted to enter the pass phrase (password) that is used to encrypt the key.
des3	<Boolean>	Read-write	Encrypt the generated RSA key by using the Triple-DES algorithm. On the command line, you are prompted to enter the pass phrase (password) that is used to encrypt the key.
aes256	<Boolean>	Read-write	Encrypt the generated RSA key by using the AES algorithm.
password	<String>	Read-write	Pass phrase to use for encryption if DES or DES3 option is selected. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum length = 31
pkcs8	<Boolean>	Read-write	Create the private key in PKCS#8 format.

Operations

(click to see Properties)

- CREATE

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

CREATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslrsakey? **action=create HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"sslrsakey":{

<b>"keyfile":<String_value>,

</b><b>"bits":<Integer_value>,

</b>"exponent":<String_value>,

"keyform":<String_value>,

"des":<Boolean_value>,

"des3":<Boolean_value>,

"aes256":<Boolean_value>,

"password":<String_value>,

"pkcs8":<Boolean_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

sslservice

Configuration for SSL service resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
servicename	<String>	Read-write	Name of the SSL service. Minimum length = 1
dh	<String>	Read-write	State of Diffie-Hellman (DH) key exchange. This parameter is not applicable when configuring a backend service. Default value: DISABLED Possible values = ENABLED, DISABLED
dhfile	<String>	Read-write	Name for and, optionally, path to the PEM-format DH parameter file to be installed. /nsconfig/ssl/ is the default path. This parameter is not applicable when configuring a backend service. Minimum length = 1
dhcount	<Integer>	Read-write	Number of interactions, between the client and the Citrix ADC, after which the DH private-public pair is regenerated. A value

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			of zero (0) specifies refresh every time. This parameter is not applicable when configuring a backend service. Allowed DH count values are 0 and >= 500. Minimum value = 0 Maximum value = 65534
dhkeyexpsizelimit	<String>	Read-write	This option enables the use of NIST recommended (NIST Special Publication 800-56A) bit size for private-key size. For example, for DH params of size 2048bit, the private-key size recommended is 224bits. This is rounded-up to 256bits. Default value: DISABLED Possible values = ENABLED, DISABLED
ersa	<String>	Read-write	State of Ephemeral RSA (eRSA) key exchange. Ephemeral RSA allows clients that support only export

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			ciphers to communicate with the secure server even if the server certificate does not support export clients. The ephemeral RSA key is automatically generated when you bind an export cipher to an SSL or TCP-based SSL virtual server or service. When you remove the export cipher, the eRSA key is not deleted. It is reused at a later date when another export cipher is bound to an SSL or TCP-based SSL virtual server or service. The eRSA key is deleted when the appliance restarts. This parameter is not applicable when configuring a backend service. Default value: DISABLED Possible values = ENABLED, DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ersacount	<Integer>	Read-write	Refresh count for regeneration of RSA public-key and private-key pair. Zero (0) specifies infinite usage (no refresh). This parameter is not applicable when configuring a backend service. Minimum value = 0 Maximum value = 65534
sessreuse	<String>	Read-write	State of session reuse. Establishing the initial handshake requires CPU-intensive public key encryption operations. With the ENABLED setting, session key exchange is avoided for session resumption requests received from the client. Default value: ENABLED Possible values = ENABLED, DISABLED
sesstimeout	<Integer>	Read-write	Time, in seconds, for which to keep the session active. Any

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			session resumption request received after the timeout period will require a fresh SSL handshake and establishment of a new SSL session. Default value: 300 Minimum value = 0 Maximum value = 4294967294
cipherredirect	<String>	Read-write	State of Cipher Redirect. If this parameter is set to ENABLED, you can configure an SSL virtual server or service to display meaningful error messages if the SSL handshake fails because of a cipher mismatch between the virtual server or service and the client. This parameter is not applicable when configuring a backend service. Default value: DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ENABLED, DISABLED
cipherurl	<String>	Read-write	URL of the page to which to redirect the client in case of a cipher mismatch. Typically, this page has a clear explanation of the error or an alternative location that the transaction can continue from. This parameter is not applicable when configuring a backend service.
sslv2redirect	<String>	Read-write	State of SSLv2 Redirect. If this parameter is set to ENABLED, you can configure an SSL virtual server or service to display meaningful error messages if the SSL handshake fails because of a protocol version mismatch between the virtual server or service and the client. This parameter is not applicable when

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			configuring a backend service. Default value: DISABLED Possible values = ENABLED, DISABLED
sslv2url	<String>	Read-write	URL of the page to which to redirect the client in case of a protocol version mismatch. Typically, this page has a clear explanation of the error or an alternative location that the transaction can continue from. This parameter is not applicable when configuring a backend service.
clientauth	<String>	Read-write	State of client authentication. In service-based SSL offload, the service terminates the SSL handshake if the SSL client does not provide a valid certificate. This parameter is not applicable when configuring a backend service.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: DISABLED Possible values = ENABLED, DISABLED
clientcert	<String>	Read-write	Type of client authentication. If this parameter is set to MANDATORY, the appliance terminates the SSL handshake if the SSL client does not provide a valid certificate. With the OPTIONAL setting, the appliance requests a certificate from the SSL clients but proceeds with the SSL transaction even if the client presents an invalid certificate. This parameter is not applicable when configuring a backend SSL service. Caution: Define proper access control policies before changing this setting to Optional. Possible values = Mandatory, Optional

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
sslredirect	<String>	Read-write	State of HTTPS redirects for the SSL service. For an SSL session, if the client browser receives a redirect message, the browser tries to connect to the new location. However, the secure SSL session breaks if the object has moved from a secure site (https://) to an unsecure site (http://). Typically, a warning message appears on the screen, prompting the user to continue or disconnect. If SSL Redirect is ENABLED, the redirect message is automatically converted from http:// to https:// and the SSL session does not break. This parameter is not applicable when configuring a backend service.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: DISABLED Possible values = ENABLED, DISABLED
redirectportrewrite	<String>	Read-write	State of the port rewrite while performing HTTPS redirect. If this parameter is set to ENABLED, and the URL from the server does not contain the standard port, the port is rewritten to the standard. Default value: DISABLED Possible values = ENABLED, DISABLED
ssl2	<String>	Read-write	State of SSLv2 protocol support for the SSL service. This parameter is not applicable when configuring a backend service. Default value: DISABLED Possible values = ENABLED, DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ssl3	<String>	Read-write	State of SSLv3 protocol support for the SSL service. Note: On platforms with SSL acceleration chips, if the SSL chip does not support SSLv3, this parameter cannot be set to ENABLED. Default value: ENABLED Possible values = ENABLED, DISABLED
tls1	<String>	Read-write	State of TLSv1.0 protocol support for the SSL service. Default value: ENABLED Possible values = ENABLED, DISABLED
tls11	<String>	Read-write	State of TLSv1.1 protocol support for the SSL service. Default value: ENABLED Possible values = ENABLED, DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
tls12	<String>	Read-write	State of TLSv1.2 protocol support for the SSL service. Default value: ENABLED Possible values = ENABLED, DISABLED
tls13	<String>	Read-write	State of TLSv1.3 protocol support for the SSL service. Default value: DISABLED Possible values = ENABLED, DISABLED
dtls1	<String>	Read-write	State of DTLSv1.0 protocol support for the SSL service. Default value: ENABLED Possible values = ENABLED, DISABLED
dtls12	<String>	Read-write	State of DTLSv1.2 protocol support for the SSL service. Default value: DISABLED Possible values = ENABLED, DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
snienable	<String>	Read-write	State of the Server Name Indication (SNI) feature on the virtual server and service-based offload. SNI helps to enable SSL encryption on multiple domains on a single virtual server or service if the domains are controlled by the same organization and share the same second-level domain name. For example, *.sports.net can be used to secure domains such as login.sports.net and help.sports.net. Default value: DISABLED Possible values = ENABLED, DISABLED
ocspstapling	<String>	Read-write	State of OCSP stapling support on the SSL virtual server. Supported only if the protocol used is higher than SSLv3. Possible values: ENABLED: The appliance sends a request to the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			OCSP responder to check the status of the server certificate and caches the response for the specified time. If the response is valid at the time of SSL handshake with the client, the OCSP-based server certificate status is sent to the client during the handshake. DISABLED: The appliance does not check the status of the server certificate. . Default value: DISABLED Possible values = ENABLED, DISABLED
serverauth	<String>	Read-write	State of server authentication support for the SSL service. Default value: DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ENABLED, DISABLED
commonname	<String>	Read-write	Name to be checked against the CommonName (CN) field in the server certificate bound to the SSL server. Minimum length = 1
pushenctrigger	<String>	Read-write	Trigger encryption on the basis of the PUSH flag value. Available settings function as follows: * ALWAYS - Any PUSH packet triggers encryption. * IGNORE - Ignore PUSH packet for triggering encryption. * MERGE - For a consecutive sequence of PUSH packets, the last PUSH packet triggers encryption. * TIMER - PUSH packet triggering encryption is delayed by the time defined in the set ssl parameter

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			command or in the Change Advanced SSL Settings dialog box. Possible values = Always, Merge, Ignore, Timer
sendclosenotify	<String>	Read-write	Enable sending SSL Close-Notify at the end of a transaction. Default value: YES Possible values = YES, NO
dtlsprofilename	<String>	Read-write	Name of the DTLS profile that contains DTLS settings for the service. Minimum length = 1 Maximum length = 127
sslprofile	<String>	Read-write	Name of the SSL profile that contains SSL settings for the service. Minimum length = 1 Maximum length = 127
strictsigdigestcheck	<String>	Read-write	Parameter indicating to check whether peer's certificate during TLS1.2 handshake is signed with one of

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			signature-hash combination supported by Citrix ADC. Default value: DISABLED Possible values = ENABLED, DISABLED
sslclientlogs	<String>	Read-write	This parameter is used to enable or disable the logging of additional information, such as the Session ID and SNI name, from SSL handshakes to the audit logs. Default value: DISABLED Possible values = ENABLED, DISABLED
strictclientekucheck	<String>	Read-write	Enable strict EKU extension check during client authentication. This can be set to DISABLED only for SSL service types Internal and Transparent. Default value: ENABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ENABLED, DISABLED
nonfipsciphers	<String>	Read-only	The state of usage of non FIPS approved ciphers. Default value: DISABLED Possible values = ENABLED, DISABLED
service	<Integer>	Read-only	.
skipcaname	<Boolean>	Read-only	The flag is used to indicate whether this particular CA certificate's CA_Name needs to be sent to the SSL client while requesting for client certificate in a SSL handshake.
dtlsflag	<Boolean>	Read-only	The flag is used to indicate whether DTLS is set or not.
quicflag	<Boolean>	Read-only	This flag is used to indicate the use of the QUIC transport protocol by a virtual server or service.
skipcacertbundle	<Boolean>	Read-only	The flag is used to indicate whether all CA_names in this particular CA

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			certificate bundle needs to be sent to the SSL client while requesting for client certificate in a SSL handshake.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslservice **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"sslservice":{

<b>"servicename":<String_value>,

</b>"dh":<String_value>,

"dhfile":<String_value>,

"dhcount":<Integer_value>,

"dhkeyexpsizelimit":<String_value>,

"ersa":<String_value>,

"ersacount":<Integer_value>,

"sessreuse":<String_value>,

"sesstimeout":<Integer_value>,

"cipherredirect":<String_value>,

"cipherurl":<String_value>,

"sslv2redirect":<String_value>,
```

```
"sslv2url":<String_value>,

"clientauth":<String_value>,

"clientcert":<String_value>,

"sslredirect":<String_value>,

"redirectportrewrite":<String_value>,

"ssl2":<String_value>,

"ssl3":<String_value>,

"tls1":<String_value>,

"tls11":<String_value>,

"tls12":<String_value>,

"tls13":<String_value>,

"dtls1":<String_value>,

"dtls12":<String_value>,

"snienable":<String_value>,

"ocspstapling":<String_value>,

"serverauth":<String_value>,

"commonname":<String_value>,

"pushenctrigger":<String_value>,

"sendclosenotify":<String_value>,

"dtlsprofilename":<String_value>,

"sslprofile":<String_value>,

"strictsigdigestcheck":<String_value>,
```

```
"sslclientlogs":<String_value>,

"strictclientekucheck":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslservice? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"sslservice":{

<b>"servicename":<String_value>,

</b>"dh":true,

"dhfile":true,

"dhcount":true,

"dhkeyexpsizelimit":true,

"ersa":true,

"ersacount":true,

"sessreuse":true,
```

```
"sesstimeout":true,

"cipherredirect":true,

"cipherurl":true,

"sslv2redirect":true,

"sslv2url":true,

"clientauth":true,

"clientcert":true,

"sslredirect":true,

"redirectportrewrite":true,

"ssl2":true,

"ssl3":true,

"tls1":true,

"tls11":true,

"tls12":true,

"tls13":true,

"dtls1":true,

"dtls12":true,

"snienable":true,

"ocspstapling":true,

"serverauth":true,

"commonname":true,

"sendclosenotify":true,
```

```
"dtlsprofilename":true,

"sslprofile":true,

"strictsigdigestcheck":true,

"sslclientlogs":true,

"strictclientekucheck":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslservice **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/sslservice? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/sslservice? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of sslservice resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/sslservice? **view=summary**

Use this query-parameter to get the summary output of sslservice resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/sslservice? **pagesize=#no;pageno=#no**

Use this query-parameter to get the sslservice resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "sslservice": [ {

"servicename":<String_value>,

"dh":<String_value>,

"dhfile":<String_value>,

"dhcount":<Integer_value>,

"dhkeyexpsizelimit":<String_value>,

"ersa":<String_value>,

"ersacount":<Integer_value>,

"sessreuse":<String_value>,

"sesstimeout":<Integer_value>,

"cipherredirect":<String_value>,

"cipherurl":<String_value>,

"sslv2redirect":<String_value>,

"sslv2url":<String_value>,
```

```
"clientauth":<String_value>,

"clientcert":<String_value>,

"sslredirect":<String_value>,

"redirectportrewrite":<String_value>,

"nonfipsciphers":<String_value>,

"ssl2":<String_value>,

"ssl3":<String_value>,

"tls1":<String_value>,

"tls11":<String_value>,

"tls12":<String_value>,

"tls13":<String_value>,

"dtls1":<String_value>,

"dtls12":<String_value>,

"snienable":<String_value>,

"ocspstapling":<String_value>,

"serverauth":<String_value>,

"commonname":<String_value>,

"service":<Integer_value>,

"pushenctrigger":<String_value>,

"skipcaname":<Boolean_value>,

"sendclosenotify":<String_value>,

"dtlsprofilename":<String_value>,
```

```
"dtlsflag":<Boolean_value>,

"quicflag":<Boolean_value>,

"sslprofile":<String_value>,

"strictsigdigestcheck":<String_value>,

"skipcacertbundle":<Boolean_value>,

"sslclientlogs":<String_value>,

"strictclientekucheck":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslservice/ servicename_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/sslservice/ servicename_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/sslservice/ servicename_value<String> ? **view=summary**

Use this query-parameter to get the summary output of sslservice resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslservice": [ {

"servicename":<String_value>,

"dh":<String_value>,

"dhfile":<String_value>,

"dhcount":<Integer_value>,

"dhkeyexpsizelimit":<String_value>,

"ersa":<String_value>,

"ersacount":<Integer_value>,

"sessreuse":<String_value>,

"sesstimeout":<Integer_value>,

"cipherredirect":<String_value>,

"cipherurl":<String_value>,

"sslv2redirect":<String_value>,

"sslv2url":<String_value>,

"clientauth":<String_value>,

"clientcert":<String_value>,

"sslredirect":<String_value>,
```

```
"redirectportrewrite":<String_value>,

"nonfipsciphers":<String_value>,

"ssl2":<String_value>,

"ssl3":<String_value>,

"tls1":<String_value>,

"tls11":<String_value>,

"tls12":<String_value>,

"tls13":<String_value>,

"dtls1":<String_value>,

"dtls12":<String_value>,

"snienable":<String_value>,

"ocspstapling":<String_value>,

"serverauth":<String_value>,

"commonname":<String_value>,

"service":<Integer_value>,

"pushenctrigger":<String_value>,

"skipcaname":<Boolean_value>,

"sendclosenotify":<String_value>,

"dtlsprofilename":<String_value>,

"dtlsflag":<Boolean_value>,

"quicflag":<Boolean_value>,

"sslprofile":<String_value>,
```

```
"strictsigdigestcheck":<String_value>,

"skipcacertbundle":<Boolean_value>,

"sslclientlogs":<String_value>,

"strictclientekucheck":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslservice? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "sslservice": [ { "__count": "#no"} ] }
```

sslservice_binding

Binding object which returns the resources bound to sslservice.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
servicename	<String>	Read-write	Name of the SSL service for which to show detailed information. Minimum length = 1
sslservice_ecccurve_binding	<sslservice_ecccurve_binding[]>	Read-only	ecccurve that can be bound to sslservice.
sslservice_sslcertkey_binding	<sslservice_sslcertkey_binding[]>	Read-only	sslcertkey that can be bound to sslservice.
sslservice_sslcipher_binding	<sslservice_sslcipher_binding[]>	Read-only	sslcipher that can be bound to sslservice.
sslservice_sslciphersuite_binding	<sslservice_sslciphersuite_binding[]>	Read-only	sslciphersuite that can be bound to sslservice.
sslservice_sslcacertbundle_binding	<sslservice_sslcacertbundle_binding[]>	Read-only	sslcacertbundle that can be bound to sslservice.
sslservice_sslpolicy_binding	<sslservice_sslpolicy_binding[]>	Read-only	sslpolicy that can be bound to sslservice.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslservice_binding/ servicename_value<String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "sslservice_binding": [ {

"servicename":<String_value>,
```

```
"sslservice_sslcertkey_binding":<sslservice_sslcertkey_binding[]_value>,

"sslservice_sslcacertbundle_binding":<sslservice_sslcacertbundle_binding[]
_value>,

"sslservice_sslciphersuite_binding":<sslservice_sslciphersuite_binding[]_v
alue>,

"sslservice_sslpolicy_binding":<sslservice_sslpolicy_binding[]_value>,

"sslservice_ecccurve_binding":<sslservice_ecccurve_binding[]_value>,

"sslservice_sslcipher_binding":<sslservice_sslcipher_binding[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslservice_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/sslservice_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "sslservice_binding": [ {

"servicename":<String_value>,

"sslservice_sslcertkey_binding":<sslservice_sslcertkey_binding[]_value>,

"sslservice_sslcacertbundle_binding":<sslservice_sslcacertbundle_binding[]
_value>,

"sslservice_sslciphersuite_binding":<sslservice_sslciphersuite_binding[]_v
alue>,

"sslservice_sslpolicy_binding":<sslservice_sslpolicy_binding[]_value>,

"sslservice_ecccurve_binding":<sslservice_ecccurve_binding[]_value>,

"sslservice_sslcipher_binding":<sslservice_sslcipher_binding[]_value>

}]}
```

sslservice_ecccurve_binding

Binding object showing the ecccurve that can be bound to sslservice.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
servicename	<String>	Read-write	Name of the SSL service for which to set advanced configuration. Minimum length = 1
ecccurvename	<String>	Read-write	Named ECC curve bound to service/ vserver. Possible values = ALL, P_224, P_256, P_384, P_521,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			X_25519, X25519_MLKEM768
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/sslservice_ecccurve_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"sslservice_ecccurve_binding":{

<b>"servicename":<String_value>,

</b>"ecccurvename":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslservice_ecccurve_binding/ servicename_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/ config/sslservice_ecccurve_binding/ servicename_value<String> ? **args=ecccurvename: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslservice_ecccurve_binding/ servicename_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/ config/sslservice_ecccurve_binding/ servicename_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of sslservice_ecccurve_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/sslservice_ecccurve_binding/ servicename_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the sslservice_ecccurve_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslservice_ecccurve_binding": [ {

"servicename":<String_value>,

"ecccurvename":<String_value>
```

```
}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslservice_ecccurve_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/sslservice_ecccurve_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslservice_ecccurve_binding": [ {

"servicename":<String_value>,

"ecccurvename":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslservice_ecccurve_binding/ servicename_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"sslservice_ecccurve_binding": [ { "__count": "#no"} ] }
```

sslservice_sslcacertbundle_binding

Binding object showing the sslcacertbundle that can be bound to sslservice.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
skipcacertbundle	<Boolean>	Read-write	The flag is used to indicate whether all CA_names in this particular CA certificate bundle needs to be sent to the SSL client while requesting for client certificate in a SSL handshake.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
servicename	<String>	Read-write	Name of the SSL service for which to set advanced configuration. Minimum length = 1
cacertbundlename	<String>	Read-write	CA certbundle name bound to the service. Minimum length = 1 Maximum length = 127
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of

creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/sslservice_sslcacertbundle_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"sslservice_sslcacertbundle_binding":{

<b>"servicename":<String_value>,

</b>"cacertbundlename":<String_value>,

"skipcacertbundle":<Boolean_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslservice_sslcacertbundle_binding/ servicename_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/ config/sslservice_sslcacertbundle_binding/ servicename_value<String> ? **args=cacertbundlename: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslservice_sslcacertbundle_binding/ servicename_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/ config/sslservice_sslcacertbundle_binding/ servicename_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of sslservice_sslcacertbundle_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/sslservice_sslcacertbundle_binding/ servicename_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the sslservice_sslcacertbundle_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslservice_sslcacertbundle_binding": [ {

"skipcacertbundle":<Boolean_value>,

"servicename":<String_value>,

"cacertbundlename":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslservice_sslcacertbundle_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/sslservice_sslcacertbundle_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslservice_sslcacertbundle_binding": [ {

"skipcacertbundle":<Boolean_value>,

"servicename":<String_value>,

"cacertbundlename":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslservice_sslcacertbundle_binding/ servicename_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"sslservice_sslcacertbundle_binding": [ { "__count": "#no"} ] }
```

sslservice_sslcertkey_binding

Binding object showing the sslcertkey that can be bound to sslservice.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
snicert	<Boolean>	Read-write	The name of the CertKey. Use this option to bind Certkey(s) which will be used in SNI processing.
crlcheck	<String>	Read-write	The state of the CRL check parameter. (Mandatory/ Optional). Possible values = Mandatory, Optional
ocspcheck	<String>	Read-write	Rule to use for the OCSP responder associated with the CA certificate during client authentication. If MANDATORY is specified, deny all SSL clients if the OCSP check fails because of connectivity issues with the remote OCSP server, or any other reason that prevents the OCSP check. With the OPTIONAL setting, allow SSL clients even if the OCSP check fails except when the client certificate is revoked.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = Mandatory, Optional
skipcaname	<Boolean>	Read-write	The flag is used to indicate whether this particular CA certificate's CA_Name needs to be sent to the SSL client while requesting for client certificate in a SSL handshake.
certkeyname	<String>	Read-write	The certificate key pair binding.
ca	<Boolean>	Read-write	CA certificate.
servicename	<String>	Read-write	Name of the SSL service for which to set advanced configuration. Minimum length = 1
cleartextport	<Integer>	Read-only	The clearTextPort settings. Minimum value = 0 Maximum value = 65534 Range 1 - 65535 * in CLI is represented as 65535 in NITRO API
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/sslservice_sslcertkey_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"sslservice_sslcertkey_binding":{

<b>"servicename":<String_value>,

</b>"certkeyname":<String_value>,

"ca":<Boolean_value>,

"crlcheck":<String_value>,

"skipcaname":<Boolean_value>,

"snicert":<Boolean_value>,

"ocspcheck":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslservice_sslcertkey_binding/ servicename_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/ config/sslservice_sslcertkey_binding/ servicename_value<String> ? **args=certkeyname: <String_value> ,ca: <Boolean_value> ,crlcheck: <String_value> ,snicert: <Boolean_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslservice_sslcertkey_binding/ servicename_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/ config/sslservice_sslcertkey_binding/ servicename_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of sslservice_sslcertkey_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/sslservice_sslcertkey_binding/ servicename_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the sslservice_sslcertkey_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslservice_sslcertkey_binding": [ {

"snicert":<Boolean_value>,

"crlcheck":<String_value>,
```

```
"ocspcheck":<String_value>,

"skipcaname":<Boolean_value>,

"certkeyname":<String_value>,

"ca":<Boolean_value>,

"servicename":<String_value>,

"cleartextport":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslservice_sslcertkey_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/sslservice_sslcertkey_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslservice_sslcertkey_binding": [ {

"snicert":<Boolean_value>,

"crlcheck":<String_value>,

"ocspcheck":<String_value>,

"skipcaname":<Boolean_value>,

"certkeyname":<String_value>,

"ca":<Boolean_value>,

"servicename":<String_value>,

"cleartextport":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslservice_sslcertkey_binding/ servicename_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"sslservice_sslcertkey_binding": [ { "__count": "#no"} ] }
```

sslservice_sslcipher_binding

Binding object showing the sslcipher that can be bound to sslservice.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
cipheraliasname	<String>	Read-write	The cipher group/ alias/individual cipher configuration.
cipherdefaulton	<Integer>	Read-write	Flag indicating whether the bound cipher was the DEFAULT cipher, bound at boot time, or any other cipher from the CLI.
description	<String>	Read-write	The cipher suite description.
servicename	<String>	Read-write	Name of the SSL service for which to set advanced configuration. Minimum length = 1
ciphername	<String>	Read-write	Name of the individual cipher, user-defined cipher group, or predefined (built-in) cipher alias.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/sslservice_sslcipher_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"sslservice_sslcipher_binding":{

<b>"servicename":<String_value>,

</b>"ciphername":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslservice_sslcipher_binding/ servicename_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/ config/sslservice_sslcipher_binding/ servicename_value<String> ? **args=ciphername: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslservice_sslcipher_binding/ servicename_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/

config/sslservice_sslcipher_binding/ servicename_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of sslservice_sslcipher_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/sslservice_sslcipher_binding/ servicename_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the sslservice_sslcipher_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslservice_sslcipher_binding": [ {

"cipheraliasname":<String_value>,

"cipherdefaulton":<Integer_value>,

"description":<String_value>,

"servicename":<String_value>,

"ciphername":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslservice_sslcipher_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/sslservice_sslcipher_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslservice_sslcipher_binding": [ {

"cipheraliasname":<String_value>,

"cipherdefaulton":<Integer_value>,

"description":<String_value>,

"servicename":<String_value>,

"ciphername":<String_value>

}]}
```

```
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslservice_sslcipher_binding/ servicename_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"sslservice_sslcipher_binding": [ { "__count": "#no"} ] }
```

sslservice_sslciphersuite_binding

Binding object showing the sslciphersuite that can be bound to sslservice.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ciphername	<String>	Read-write	The cipher group/ alias/individual cipher configuration.
servicename	<String>	Read-write	Name of the SSL service for which to set advanced configuration.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum length = 1
description	<String>	Read-write	The cipher suite description.
cipherdefaulton	<Integer>	Read-write	Flag indicating whether the bound cipher was the DEFAULT cipher, bound at boot time, or any other cipher from the CLI.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/sslservice_sslciphersuite_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"sslservice_sslciphersuite_binding":{

<b>"servicename":<String_value>,

</b>"ciphername":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslservice_sslciphersuite_binding/ servicename_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/ config/sslservice_sslciphersuite_binding/ servicename_value<String> ? **args=ciphername: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslservice_sslciphersuite_binding/ servicename_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/ config/sslservice_sslciphersuite_binding/ servicename_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of sslservice_sslciphersuite_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/sslservice_sslciphersuite_binding/ servicename_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the sslservice_sslciphersuite_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslservice_sslciphersuite_binding": [ {

"ciphername":<String_value>,

"servicename":<String_value>,

"description":<String_value>,

"cipherdefaulton":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslservice_sslciphersuite_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/sslservice_sslciphersuite_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslservice_sslciphersuite_binding": [ {

"ciphername":<String_value>,

"servicename":<String_value>,

"description":<String_value>,

"cipherdefaulton":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslservice_sslciphersuite_binding/ servicename_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"sslservice_sslciphersuite_binding": [ { "__count": "#no"} ] }
```

sslservice_sslpolicy_binding

Binding object showing the sslpolicy that can be bound to sslservice.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
invoke	<Boolean>	Read-write	Invoke flag. This attribute is relevant only for ADVANCED policies.
gotopriorityexpression	<String>	Read-write	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
policyname	<String>	Read-write	The SSL policy binding.
servicename	<String>	Read-write	Name of the SSL service for which to set advanced configuration. Minimum length = 1
type	<String>	Read-write	The phase of the SSL connection in which the policy rule is evaluated. Possible Value: SERVER_AUTH_VAL_REQ. The bindpoint means:: 1. SERVER_AUTH_VAL_REQ: Policy evaluation will be performed during the verification of the server certificate. Action allowed with this type is:

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			OCSPCERTVALIDATION. Possible values = SERVER_AUTH_VAL
labelname	<String>	Read-write	Name of the label to invoke if the current policy rule evaluates to TRUE.
priority	<Integer>	Read-write	The priority of the policies bound to this SSL service. Minimum value = 0 Maximum value = 65534
labeltype	<String>	Read-write	Type of policy label invocation. Possible values = vserver, service, policylabel
polinherit	<Integer>	Read-only	Whether the bound policy is a inherited policy or not. Minimum value = 0 Maximum value = 254
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD

- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/sslservice_sslpolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"sslservice_sslpolicy_binding":{

<b>"servicename":<String_value>,

</b>"policyname":<String_value>,

"priority":<Integer_value>,

"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>,

"labeltype":<String_value>,

"labelname":<String_value>,

"type":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslservice_sslpolicy_binding/ servicename_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/ config/sslservice_sslpolicy_binding/ servicename_value<String> ? **args=policyname: <String_value> ,priority: <Integer_value> ,type: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslservice_sslpolicy_binding/ servicename_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/ config/sslservice_sslpolicy_binding/ servicename_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of sslservice_sslpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/sslservice_sslpolicy_binding/ servicename_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the sslservice_sslpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslservice_sslpolicy_binding": [ {

"invoke":<Boolean_value>,

"gotopriorityexpression":<String_value>,

"policyname":<String_value>,
```

```
"servicename":<String_value>,

"type":<String_value>,

"labelname":<String_value>,

"priority":<Integer_value>,

"labeltype":<String_value>,

"polinherit":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslservice_sslpolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/sslservice_sslpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslservice_sslpolicy_binding": [ {

"invoke":<Boolean_value>,

"gotopriorityexpression":<String_value>,

"policyname":<String_value>,

"servicename":<String_value>,

"type":<String_value>,

"labelname":<String_value>,

"priority":<Integer_value>,

"labeltype":<String_value>,

"polinherit":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslservice_sslpolicy_binding/ servicename_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"sslservice_sslpolicy_binding": [ { "__count": "#no"} ] }
```

sslservicegroup

Configuration for SSL service group resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
servicegroupname	<String>	Read-write	Name of the SSL service group for which to set advanced configuration. Minimum length = 1
sslprofile	<String>	Read-write	Name of the SSL profile that contains SSL settings for the Service Group. Minimum length = 1 Maximum length = 127
sessreuse	<String>	Read-write	State of session reuse. Establishing the initial handshake requires CPU-intensive public key encryption operations. With the ENABLED setting, session key exchange is avoided for session resumption requests received from the client.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: ENABLED Possible values = ENABLED, DISABLED
sesstimeout	<Integer>	Read-write	Time, in seconds, for which to keep the session active. Any session resumption request received after the timeout period will require a fresh SSL handshake and establishment of a new SSL session. Default value: 300 Minimum value = 0 Maximum value = 4294967294
ssl3	<String>	Read-write	State of SSLv3 protocol support for the SSL service group. Note: On platforms with SSL acceleration chips, if the SSL chip does not support SSLv3, this parameter cannot be set to ENABLED.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: ENABLED Possible values = ENABLED, DISABLED
tls1	<String>	Read-write	State of TLSv1.0 protocol support for the SSL service group. Default value: ENABLED Possible values = ENABLED, DISABLED
tls11	<String>	Read-write	State of TLSv1.1 protocol support for the SSL service group. Default value: ENABLED Possible values = ENABLED, DISABLED
tls12	<String>	Read-write	State of TLSv1.2 protocol support for the SSL service group. Default value: ENABLED Possible values = ENABLED, DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
tls13	<String>	Read-write	State of TLSv1.3 protocol support for the SSL service group. Default value: DISABLED Possible values = ENABLED, DISABLED
snienable	<String>	Read-write	State of the Server Name Indication (SNI) feature on the service. SNI helps to enable SSL encryption on multiple domains on a single virtual server or service if the domains are controlled by the same organization and share the same second-level domain name. For example, *.sports.net can be used to secure domains such as login.sports.net and help.sports.net. Default value: DISABLED Possible values = ENABLED, DISABLED
ocspstapling	<String>	Read-write	State of OCSP stapling support on

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			the SSL virtual server. Supported only if the protocol used is higher than SSLv3. Possible values: ENABLED: The appliance sends a request to the OCSP responder to check the status of the server certificate and caches the response for the specified time. If the response is valid at the time of SSL handshake with the client, the OCSP-based server certificate status is sent to the client during the handshake. DISABLED: The appliance does not check the status of the server certificate. Default value: DISABLED Possible values = ENABLED, DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
serverauth	<String>	Read-write	State of server authentication support for the SSL service group. Default value: DISABLED Possible values = ENABLED, DISABLED
commonname	<String>	Read-write	Name to be checked against the CommonName (CN) field in the server certificate bound to the SSL server. Minimum length = 1
sendclosenotify	<String>	Read-write	Enable sending SSL Close-Notify at the end of a transaction. Default value: YES Possible values = YES, NO
strictsigdigestcheck	<String>	Read-write	Parameter indicating to check whether peer's certificate is signed with one of signature-hash combination supported by Citrix ADC. Default value: DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ENABLED, DISABLED
sslclientlogs	<String>	Read-write	This parameter is used to enable or disable the logging of additional information, such as the Session ID and SNI names, from SSL handshakes to the audit logs. Default value: DISABLED Possible values = ENABLED, DISABLED
dh	<String>	Read-only	The state of DH key exchange support for the SSL service group. Possible values = ENABLED, DISABLED
dhfile	<String>	Read-only	The file name and path for the DH parameter.
dhcount	<Integer>	Read-only	The refresh count for the re-generation of DH public-key and private-key from the DH parameter. Minimum value = 0

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum value = 65534
dhkeyexpsizelimit	<String>	Read-only	This option enables the use of NIST recommended (NIST Special Publication 800-56A) bit size for private-key size. For example, for DH params of size 2048bit, the private-key size recommended is 224bits. This is rounded-up to 256bits. Possible values = ENABLED, DISABLED
ersa	<String>	Read-only	The state of Ephemeral RSA key exchange support for the SSL service group.Ephemeral RSA is used for export ciphers. Possible values = ENABLED, DISABLED
ersacount	<Integer>	Read-only	The refresh count for the re-generation of RSA public-key and private-key pair. Minimum value = 0 Maximum value = 65534

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
cipherredirect	<String>	Read-only	The state of Cipher Redirect feature. Cipher Redirect feature can be used to provide more readable information to SSL clients about mismatch in ciphers between the client and the SSL vserver. Possible values = ENABLED, DISABLED
cipherurl	<String>	Read-only	The redirect URL to be used with the Cipher Redirect feature.
sslv2redirect	<String>	Read-only	The state of SSLv2 Redirect feature.SSLv2 Redirect feature can be used to provide more readable information to SSL client about non-support of SSLv2 protocol on the SSL vserver. Possible values = ENABLED, DISABLED
sslv2url	<String>	Read-only	The redirect URL to be used with SSLv2 Redirect feature.
clientauth	<String>	Read-only	The state of Client-Authentication

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			support for the SSL service group. Possible values = ENABLED, DISABLED
clientcert	<String>	Read-only	The rule for client certificate requirement in client authentication. Possible values = Mandatory, Optional
sslredirect	<String>	Read-only	The state of HTTPS redirects for the SSL service group. This is required for the proper functioning of the redirect messages from the server. The redirect message from the server provides the new location for the moved object. This is contained in the HTTP header field: Location, e.g. Location: http://www.moved.org/here.html For the SSL session, if the client browser receives this message, the browser will try to

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			connect to the new location. This will break the secure SSL session, as the object has moved from a secure site (https://) to an un-secure one (http://). Generally browsers flash a warning message on the screen and prompt the user, either to continue or disconnect. The above feature, when enabled will automatically convert all such http:// redirect message to https://. This will not break the client SSL session. Note: The set ssl service command can be used for configuring a front-end SSL service for service based SSL Off-Loading, or a backend SSL service for backend-encryption setup.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ENABLED, DISABLED
redirectportrewrite	<String>	Read-only	The state of port-rewrite feature. Possible values = ENABLED, DISABLED
nonfipsciphers	<String>	Read-only	The state of usage of non FIPS approved ciphers. Default value: DISABLED Possible values = ENABLED, DISABLED
ssl2	<String>	Read-only	The state of SSLv2 protocol support for the SSL service group. Possible values = ENABLED, DISABLED
ocspcheck	<String>	Read-only	The state of the OCSP check parameter. (Mandatory/ Optional). Possible values = Mandatory, Optional
crlcheck	<String>	Read-only	The state of the CRL check parameter.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			(Mandatory/ Optional). Possible values = Mandatory, Optional
cleartextport	<Integer>	Read-only	The port on the back-end web-servers where the clear-text data is sent by system. Use this setting for the wildcard IP based SSL Acceleration configuration (*:443). Minimum value = 0 Maximum value = 65534 Range 1 - 65535 * in CLI is represented as 65535 in NITRO API
servicename	<String>	Read-only	The service name.
ca	<Boolean>	Read-only	CA certificate.
snicert	<Boolean>	Read-only	The name of the CertKey. Use this option to bind Certkey(s) which will be used in SNI processing.
quicflag	<Boolean>	Read-only	This flag is used to indicate the use of the QUIC transport

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			protocol by a virtual server or service.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslservicegroup **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"sslservicegroup":{

<b>"servicegroupname":<String_value>,

</b>"sslprofile":<String_value>,

"sessreuse":<String_value>,

"sesstimeout":<Integer_value>,

"ssl3":<String_value>,

"tls1":<String_value>,

"tls11":<String_value>,

"tls12":<String_value>,

"tls13":<String_value>,

"snienable":<String_value>,

"ocspstapling":<String_value>,

"serverauth":<String_value>,

"commonname":<String_value>,

"sendclosenotify":<String_value>,
```

```
"strictsigdigestcheck":<String_value>,

"sslclientlogs":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslservicegroup? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"sslservicegroup":{

<b>"servicegroupname":<String_value>,

</b>"sslprofile":true,

"sessreuse":true,

"sesstimeout":true,

"ssl3":true,

"tls1":true,

"tls11":true,

"tls12":true,
```

```
"tls13":true,

"snienable":true,

"ocspstapling":true,

"serverauth":true,

"commonname":true,

"sendclosenotify":true,

"strictsigdigestcheck":true,

"sslclientlogs":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslservicegroup **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/sslservicegroup? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/sslservicegroup? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of sslservicegroup resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/sslservicegroup? **view=summary**

Use this query-parameter to get the summary output of sslservicegroup resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/sslservicegroup? **pagesize=#no;pageno=#no**

Use this query-parameter to get the sslservicegroup resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "sslservicegroup": [ {

"servicegroupname":<String_value>,

"dh":<String_value>,

"dhfile":<String_value>,

"dhcount":<Integer_value>,

"dhkeyexpsizelimit":<String_value>,

"ersa":<String_value>,

"ersacount":<Integer_value>,

"sessreuse":<String_value>,

"sesstimeout":<Integer_value>,
```

```
"cipherredirect":<String_value>,

"cipherurl":<String_value>,

"sslv2redirect":<String_value>,

"sslv2url":<String_value>,

"clientauth":<String_value>,

"clientcert":<String_value>,

"sslredirect":<String_value>,

"redirectportrewrite":<String_value>,

"nonfipsciphers":<String_value>,

"ssl2":<String_value>,

"ssl3":<String_value>,

"tls1":<String_value>,

"tls11":<String_value>,

"tls12":<String_value>,

"tls13":<String_value>,

"snienable":<String_value>,

"ocspstapling":<String_value>,

"serverauth":<String_value>,

"commonname":<String_value>,

"ocspcheck":<String_value>,

"crlcheck":<String_value>,

"cleartextport":<Integer_value>,
```

```
"servicename":<String_value>,

"ca":<Boolean_value>,

"snicert":<Boolean_value>,

"sendclosenotify":<String_value>,

"quicflag":<Boolean_value>,

"sslprofile":<String_value>,

"strictsigdigestcheck":<String_value>,

"sslclientlogs":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslservicegroup/ servicegroupname_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/sslservicegroup/ servicegroupname_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/sslservicegroup/ servicegroupname_value<String> ? **view=summary**

Use this query-parameter to get the summary output of sslservicegroup resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslservicegroup": [ {

"servicegroupname":<String_value>,

"dh":<String_value>,

"dhfile":<String_value>,

"dhcount":<Integer_value>,

"dhkeyexpsizelimit":<String_value>,

"ersa":<String_value>,

"ersacount":<Integer_value>,

"sessreuse":<String_value>,

"sesstimeout":<Integer_value>,

"cipherredirect":<String_value>,

"cipherurl":<String_value>,

"sslv2redirect":<String_value>,

"sslv2url":<String_value>,

"clientauth":<String_value>,

"clientcert":<String_value>,
```

```
"sslredirect":<String_value>,

"redirectportrewrite":<String_value>,

"nonfipsciphers":<String_value>,

"ssl2":<String_value>,

"ssl3":<String_value>,

"tls1":<String_value>,

"tls11":<String_value>,

"tls12":<String_value>,

"tls13":<String_value>,

"snienable":<String_value>,

"ocspstapling":<String_value>,

"serverauth":<String_value>,

"commonname":<String_value>,

"ocspcheck":<String_value>,

"crlcheck":<String_value>,

"cleartextport":<Integer_value>,

"servicename":<String_value>,

"ca":<Boolean_value>,

"snicert":<Boolean_value>,

"sendclosenotify":<String_value>,

"quicflag":<Boolean_value>,

"sslprofile":<String_value>,
```

```
"strictsigdigestcheck":<String_value>,

"sslclientlogs":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslservicegroup? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "sslservicegroup": [ { "__count": "#no"} ] }
```

sslservicegroup_binding

Binding object which returns the resources bound to sslservicegroup.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
servicegroupname	<String>	Read-write	Name of the SSL service group for which to show detailed information. Minimum length = 1
sslservicegroup_sslcipher_binding	<sslservicegroup_sslcipher_binding[]>	Read-only	sslcipher that can be bound to sslservicegroup.
sslservicegroup_eccurve_binding	<sslservicegroup_eccurve_binding[]>	Read-only	ecccurve that can be bound to sslservicegroup.
sslservicegroup_sslcertkey_binding	<sslservicegroup_sslcertkey_binding[]>	Read-only	sslcertkey that can be bound to sslservicegroup.
sslservicegroup_sslciphersuite_binding	<sslservicegroup_sslciphersuite_binding[]>	Read-only	sslciphersuite that can be bound to sslservicegroup.
sslservicegroup_sslcacertbundle_binding	<sslservicegroup_sslcacertbundle_binding[]>	Read-only	sslcacertbundle that can be bound to sslservicegroup.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslservicegroup_binding/ servicegroupname_value<String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "sslservicegroup_binding": [ {

"servicegroupname":<String_value>,
```

```
"sslservicegroup_sslcacertbundle_binding":<sslservicegroup_sslcacertbundle
_binding[]_value>,

"sslservicegroup_ecccurve_binding":<sslservicegroup_ecccurve_binding[]_val
ue>,

"sslservicegroup_sslcertkey_binding":<sslservicegroup_sslcertkey_binding[]
_value>,

"sslservicegroup_sslcipher_binding":<sslservicegroup_sslcipher_binding[]_v
alue>,

"sslservicegroup_sslciphersuite_binding":<sslservicegroup_sslciphersuite_b
inding[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslservicegroup_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/sslservicegroup_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "sslservicegroup_binding": [ {

"servicegroupname":<String_value>,

"sslservicegroup_sslcacertbundle_binding":<sslservicegroup_sslcacertbundle
_binding[]_value>,

"sslservicegroup_ecccurve_binding":<sslservicegroup_ecccurve_binding[]_val
ue>,

"sslservicegroup_sslcertkey_binding":<sslservicegroup_sslcertkey_binding[]
_value>,

"sslservicegroup_sslcipher_binding":<sslservicegroup_sslcipher_binding[]_v
alue>,

"sslservicegroup_sslciphersuite_binding":<sslservicegroup_sslciphersuite_b
inding[]_value>

}]}
```

sslservicegroup_ecccurve_binding

Binding object showing the ecccurve that can be bound to sslservicegroup.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
servicegroupname	<String>	Read-write	The name of the SSL service to which the SSL policy needs to be bound. Minimum length = 1
ecccurvename	<String>	Read-write	Named ECC curve bound to servicegroup.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ALL, P_224, P_256, P_384, P_521, X_25519, X25519_MLKEM768
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/sslservicegroup_ecccurve_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"sslservicegroup_ecccurve_binding":{

<b>"servicegroupname":<String_value>,

</b>"ecccurvename":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslservicegroup_ecccurve_binding/ servicegroupname_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/sslservicegroup_ecccurve_binding/ servicegroupname_value<String> ? **args=ecccurvename: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslservicegroup_ecccurve_binding/ servicegroupname_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/sslservicegroup_ecccurve_binding/ servicegroupname_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of sslservicegroup_ecccurve_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/sslservicegroup_ecccurve_binding/ servicegroupname_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the sslservicegroup_ecccurve_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslservicegroup_ecccurve_binding": [ {

"servicegroupname":<String_value>,

"ecccurvename":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslservicegroup_ecccurve_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/sslservicegroup_ecccurve_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslservicegroup_ecccurve_binding": [ {

"servicegroupname":<String_value>,

"ecccurvename":<String_value>
```

```
}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslservicegroup_ecccurve_binding/servicegroupname_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"sslservicegroup_ecccurve_binding": [ { "__count": "#no"} ] }
```

sslservicegroup_sslcacertbundle_binding

Binding object showing the sslcacertbundle that can be bound to sslservicegroup.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
servicegroupname	<String>	Read-write	The name of the SSL service to which the SSL policy needs to be bound. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
cacertbundlename	<String>	Read-write	CA certbundle name bound to the servicegroup. Minimum length = 1 Maximum length = 127
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/sslservicegroup_sslcacertbundle_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"sslservicegroup_sslcacertbundle_binding":{

<b>"servicegroupname":<String_value>,

</b>"cacertbundlename":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslservicegroup_sslcacertbundle_binding/ servicegroupname_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/sslservicegroup_sslcacertbundle_binding/ servicegroupname_value<String> ? **args=cacertbundlename: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslservicegroup_sslcacertbundle_binding/ servicegroupname_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/sslservicegroup_sslcacertbundle_binding/ servicegroupname_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of sslservicegroup_sslcacertbundle_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ sslservicegroup_sslcacertbundle_binding/ servicegroupname_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the sslservicegroup_sslcacertbundle_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslservicegroup_sslcacertbundle_binding": [ {

"servicegroupname":<String_value>,

"cacertbundlename":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslservicegroup_sslcacertbundle_binding
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/sslservicegroup_sslcacertbundle_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslservicegroup_sslcacertbundle_binding": [ {

"servicegroupname":<String_value>,

"cacertbundlename":<String_value>
```

```
}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslservicegroup_sslcacertbundle_binding/servicegroupname_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"sslservicegroup_sslcacertbundle_binding": [ { "__count": "#no"} ] }
```

sslservicegroup_sslcertkey_binding

Binding object showing the sslcertkey that can be bound to sslservicegroup.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ca	<Boolean>	Read-write	CA certificate.
certkeyname	<String>	Read-write	The name of the certificate bound to the SSL service group.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ocspcheck	<String>	Read-write	The state of the OCSP check parameter. (Mandatory/ Optional). Possible values = Mandatory, Optional
crlcheck	<String>	Read-write	The state of the CRL check parameter. (Mandatory/ Optional). Possible values = Mandatory, Optional
snicert	<Boolean>	Read-write	The name of the CertKey. Use this option to bind Certkey(s) which will be used in SNI processing.
servicegroupname	<String>	Read-write	The name of the SSL service to which the SSL policy needs to be bound. Minimum length = 1
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/sslservicegroup_sslcertkey_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"sslservicegroup_sslcertkey_binding":{
```

```
<b>"servicegroupname":<String_value>,

</b>"certkeyname":<String_value>,

"ca":<Boolean_value>,

"crlcheck":<String_value>,

"snicert":<Boolean_value>,

"ocspcheck":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslservicegroup_sslcertkey_binding/ servicegroupname_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/sslservicegroup_sslcertkey_binding/ servicegroupname_value<String> ? **args=certkeyname: <String_value> ,ca: <Boolean_value> ,crlcheck: <String_value> ,snicert: <Boolean_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslservicegroup_sslcertkey_binding/ servicegroupname_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/

v1/config/sslservicegroup_sslcertkey_binding/ servicegroupname_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of sslservicegroup_sslcertkey_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/sslservicegroup_sslcertkey_binding/ servicegroupname_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the sslservicegroup_sslcertkey_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslservicegroup_sslcertkey_binding": [ {

"ca":<Boolean_value>,

"certkeyname":<String_value>,

"ocspcheck":<String_value>,

"crlcheck":<String_value>,

"snicert":<Boolean_value>,

"servicegroupname":<String_value>
```

```
}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslservicegroup_sslcertkey_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/sslservicegroup_sslcertkey_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslservicegroup_sslcertkey_binding": [ {

"ca":<Boolean_value>,

"certkeyname":<String_value>,

"ocspcheck":<String_value>,

"crlcheck":<String_value>,

"snicert":<Boolean_value>,
```

```
"servicegroupname":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslservicegroup_sslcertkey_binding/servicegroupname_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"sslservicegroup_sslcertkey_binding": [ { "__count": "#no"} ] }
```

sslservicegroup_sslcipher_binding

Binding object showing the sslcipher that can be bound to sslservicegroup.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
servicegroupname	<String>	Read-write	The name of the SSL service to which the SSL policy needs to be bound.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum length = 1
ciphername	<String>	Read-write	A cipher-suite can consist of an individual cipher name, the system predefined cipher-alias name, or user defined cipher-group name.
description	<String>	Read-write	The description of the cipher.
cipheraliasname	<String>	Read-write	The name of the cipher group/alias/ name configured for the SSL service group.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/sslservicegroup_sslcipher_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"sslservicegroup_sslcipher_binding":{

<b>"servicegroupname":<String_value>,

</b>"ciphername":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslservicegroup_sslcipher_binding/ servicegroupname_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/sslservicegroup_sslcipher_binding/ servicegroupname_value<String> ? **args=ciphername: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslservicegroup_sslcipher_binding/ servicegroupname_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/sslservicegroup_sslcipher_binding/ servicegroupname_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of sslservicegroup_sslcipher_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/sslservicegroup_sslcipher_binding/ servicegroupname_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the sslservicegroup_sslcipher_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslservicegroup_sslcipher_binding": [ {

"servicegroupname":<String_value>,

"ciphername":<String_value>,

"description":<String_value>,

"cipheraliasname":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslservicegroup_sslcipher_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/sslservicegroup_sslcipher_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslservicegroup_sslcipher_binding": [ {

"servicegroupname":<String_value>,

"ciphername":<String_value>,

"description":<String_value>,

"cipheraliasname":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslservicegroup_sslcipher_binding/servicegroupname_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"sslservicegroup_sslcipher_binding": [ { "__count": "#no"} ] }
```

sslservicegroup_sslciphersuite_binding

Binding object showing the sslciphersuite that can be bound to sslservicegroup.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
servicegroupname	<String>	Read-write	The name of the SSL service to which the SSL policy needs to be bound. Minimum length = 1
description	<String>	Read-write	The description of the cipher.
ciphername	<String>	Read-write	The name of the cipher group/alias/ name configured for the SSL service group.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/sslservicegroup_sslciphersuite_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"sslservicegroup_sslciphersuite_binding":{

<b>"servicegroupname":<String_value>,
```

```
</b>"ciphername":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslservicegroup_sslciphersuite_binding/ servicegroupname_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/sslservicegroup_sslciphersuite_binding/ servicegroupname_value<String> ? **args=ciphername: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslservicegroup_sslciphersuite_binding/ servicegroupname_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/sslservicegroup_sslciphersuite_binding/ servicegroupname_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of sslservicegroup_sslciphersuite_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/sslservicegroup_sslciphersuite_binding/ servicegroupname_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the sslservicegroup_sslciphersuite_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslservicegroup_sslciphersuite_binding": [ {

"servicegroupname":<String_value>,

"description":<String_value>,

"ciphername":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslservicegroup_sslciphersuite_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/sslservicegroup_sslciphersuite_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslservicegroup_sslciphersuite_binding": [ {

"servicegroupname":<String_value>,

"description":<String_value>,

"ciphername":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslservicegroup_sslciphersuite_binding/servicegroupname_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"sslservicegroup_sslciphersuite_binding": [ { "__count": "#no"} ] }
```

sslvserver

Configuration for SSL virtual server resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
vservername	<String>	Read-write	Name of the SSL virtual server for which to set advanced configuration. Minimum length = 1
cleartextport	<Integer>	Read-write	Port on which clear-text data is sent by the appliance to the server. Do not specify this parameter for SSL offloading with end-to-end encryption. Default value: 0 Minimum value = 0 Maximum value = 65534
dh	<String>	Read-write	State of Diffie-Hellman (DH) key exchange. Default value: DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ENABLED, DISABLED
dhfile	<String>	Read-write	Name of and, optionally, path to the DH parameter file, in PEM format, to be installed. /nsconfig/ssl/ is the default path. Minimum length = 1
dhcount	<Integer>	Read-write	Number of interactions, between the client and the Citrix ADC, after which the DH private-public pair is regenerated. A value of zero (0) specifies refresh every time. Minimum value = 0 Maximum value = 65534
dhkeyexpsizelimit	<String>	Read-write	This option enables the use of NIST recommended (NIST Special Publication 800-56A) bit size for private-key size. For example, for DH params of size 2048bit, the private-key size recommended is 224bits. This is

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			rounded-up to 256bits. Default value: DISABLED Possible values = ENABLED, DISABLED
ersa	<String>	Read-write	State of Ephemeral RSA (eRSA) key exchange. Ephemeral RSA allows clients that support only export ciphers to communicate with the secure server even if the server certificate does not support export clients. The ephemeral RSA key is automatically generated when you bind an export cipher to an SSL or TCP-based SSL virtual server or service. When you remove the export cipher, the eRSA key is not deleted. It is reused at a later date when another export cipher is bound to an SSL or TCP-based SSL virtual server or service. The eRSA key is deleted when

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			the appliance restarts. Default value: ENABLED Possible values = ENABLED, DISABLED
ersacount	<Integer>	Read-write	Refresh count for regeneration of the RSA public-key and private-key pair. Zero (0) specifies infinite usage (no refresh). Minimum value = 0 Maximum value = 65534
sessreuse	<String>	Read-write	State of session reuse. Establishing the initial handshake requires CPU-intensive public key encryption operations. With the ENABLED setting, session key exchange is avoided for session resumption requests received from the client. Default value: ENABLED Possible values = ENABLED, DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
sesstimeout	<Integer>	Read-write	Time, in seconds, for which to keep the session active. Any session resumption request received after the timeout period will require a fresh SSL handshake and establishment of a new SSL session. Default value: 120 Minimum value = 0 Maximum value = 4294967294
cipherredirect	<String>	Read-write	State of Cipher Redirect. If cipher redirect is enabled, you can configure an SSL virtual server or service to display meaningful error messages if the SSL handshake fails because of a cipher mismatch between the virtual server or service and the client. Default value: DISABLED Possible values = ENABLED, DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
cipherurl	<String>	Read-write	The redirect URL to be used with the Cipher Redirect feature.
sslv2redirect	<String>	Read-write	State of SSLv2 Redirect. If SSLv2 redirect is enabled, you can configure an SSL virtual server or service to display meaningful error messages if the SSL handshake fails because of a protocol version mismatch between the virtual server or service and the client. Default value: DISABLED Possible values = ENABLED, DISABLED
sslv2url	<String>	Read-write	URL of the page to which to redirect the client in case of a protocol version mismatch. Typically, this page has a clear explanation of the error or an alternative location that the transaction can continue from.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
clientauth	<String>	Read-write	State of client authentication. If client authentication is enabled, the virtual server terminates the SSL handshake if the SSL client does not provide a valid certificate. Default value: DISABLED Possible values = ENABLED, DISABLED
clientcert	<String>	Read-write	Type of client authentication. If this parameter is set to MANDATORY, the appliance terminates the SSL handshake if the SSL client does not provide a valid certificate. With the OPTIONAL setting, the appliance requests a certificate from the SSL clients but proceeds with the SSL transaction even if the client presents an invalid certificate. Caution: Define proper access control policies

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			before changing this setting to Optional. Possible values = Mandatory, Optional
sslredirect	<String>	Read-write	State of HTTPS redirects for the SSL virtual server. For an SSL session, if the client browser receives a redirect message, the browser tries to connect to the new location. However, the secure SSL session breaks if the object has moved from a secure site (https://) to an unsecure site (http://). Typically, a warning message appears on the screen, prompting the user to continue or disconnect. If SSL Redirect is ENABLED, the redirect message is automatically converted from http:// to https:// and

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			the SSL session does not break. Default value: DISABLED Possible values = ENABLED, DISABLED
redirectportrewrite	<String>	Read-write	State of the port rewrite while performing HTTPS redirect. If this parameter is ENABLED and the URL from the server does not contain the standard port, the port is rewritten to the standard. Default value: DISABLED Possible values = ENABLED, DISABLED
ssl2	<String>	Read-write	State of SSLv2 protocol support for the SSL Virtual Server. Default value: DISABLED Possible values = ENABLED, DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ssl3	<String>	Read-write	State of SSLv3 protocol support for the SSL Virtual Server. Note: On platforms with SSL acceleration chips, if the SSL chip does not support SSLv3, this parameter cannot be set to ENABLED. Default value: ENABLED Possible values = ENABLED, DISABLED
tls1	<String>	Read-write	State of TLSv1.0 protocol support for the SSL Virtual Server. Default value: ENABLED Possible values = ENABLED, DISABLED
tls11	<String>	Read-write	State of TLSv1.1 protocol support for the SSL Virtual Server. Default value: ENABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ENABLED, DISABLED
tls12	<String>	Read-write	State of TLSv1.2 protocol support for the SSL Virtual Server. Default value: ENABLED Possible values = ENABLED, DISABLED
tls13	<String>	Read-write	State of TLSv1.3 protocol support for the SSL Virtual Server. Default value: DISABLED Possible values = ENABLED, DISABLED
dtls1	<String>	Read-write	State of DTLSv1.0 protocol support for the SSL Virtual Server. Default value: ENABLED Possible values = ENABLED, DISABLED
dtls12	<String>	Read-write	State of DTLSv1.2 protocol support for

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			the SSL Virtual Server. Default value: DISABLED Possible values = ENABLED, DISABLED
snienable	<String>	Read-write	State of the Server Name Indication (SNI) feature on the virtual server and service-based offload. SNI helps to enable SSL encryption on multiple domains on a single virtual server or service if the domains are controlled by the same organization and share the same second-level domain name. For example, *.sports.net can be used to secure domains such as login.sports.net and help.sports.net. Default value: DISABLED Possible values = ENABLED, DISABLED
ocspstapling	<String>	Read-write	State of OCSP stapling support on

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			the SSL virtual server. Supported only if the protocol used is higher than SSLv3. Possible values: ENABLED: The appliance sends a request to the OCSP responder to check the status of the server certificate and caches the response for the specified time. If the response is valid at the time of SSL handshake with the client, the OCSP-based server certificate status is sent to the client during the handshake. DISABLED: The appliance does not check the status of the server certificate. . Default value: DISABLED Possible values = ENABLED, DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
pushenctrigger	<String>	Read-write	Trigger encryption on the basis of the PUSH flag value. Available settings function as follows: * ALWAYS - Any PUSH packet triggers encryption. * IGNORE - Ignore PUSH packet for triggering encryption. * MERGE - For a consecutive sequence of PUSH packets, the last PUSH packet triggers encryption. * TIMER - PUSH packet triggering encryption is delayed by the time defined in the set ssl parameter command or in the Change Advanced SSL Settings dialog box. Possible values = Always, Merge, Ignore, Timer

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
sendclosenotify	<String>	Read-write	Enable sending SSL Close-Notify at the end of a transaction. Default value: YES Possible values = YES, NO
dtlsprofilename	<String>	Read-write	Name of the DTLS profile whose settings are to be applied to the virtual server. Minimum length = 1 Maximum length = 127
sslprofile	<String>	Read-write	Name of the SSL profile that contains SSL settings for the virtual server. Minimum length = 1 Maximum length = 127
hsts	<String>	Read-write	State of HSTS protocol support for the SSL Virtual Server. Using HSTS, a server can enforce the use of an HTTPS connection for all communication with a client. Default value: DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ENABLED, DISABLED
maxage	<Integer>	Read-write	Set the maximum time, in seconds, in the strict transport security (STS) header during which the client must send only HTTPS requests to the server. Default value: 0 Minimum value = 0 Maximum value = 4294967294
includesubdomains	<String>	Read-write	Enable HSTS for subdomains. If set to Yes, a client must send only HTTPS requests for subdomains. Default value: NO Possible values = YES, NO
preload	<String>	Read-write	Flag indicates the consent of the site owner to have their domain preloaded. Default value: NO Possible values = YES, NO

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
strictsigdigestcheck	<String>	Read-write	Parameter indicating to check whether peer entity certificate during TLS1.2 handshake is signed with one of signature-hash combination supported by Citrix ADC. Default value: DISABLED Possible values = ENABLED, DISABLED
zerorttearlydata	<String>	Read-write	State of TLS 1.3 0-RTT early data support for the SSL Virtual Server. This setting only has an effect if resumption is enabled, as early data cannot be sent along with an initial handshake. Early application data has significantly different security properties - in particular there is no guarantee that the data cannot be replayed.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: DISABLED Possible values = ENABLED, DISABLED
tls13sessionticketsperauthcontext	<Integer>	Read-write	Number of tickets the SSL Virtual Server will issue anytime TLS 1.3 is negotiated, ticket-based resumption is enabled, and either (1) a handshake completes or (2) post-handhsake client auth completes. This value can be increased to enable clients to open multiple parallel connections using a fresh ticket for each connection. No tickets are sent if resumption is disabled. Default value: 1 Minimum value = 1 Maximum value = 10
dhekeyexchangewithpsk	<String>	Read-write	Whether or not the SSL Virtual Server

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			will require a DHE key exchange to occur when a PSK is accepted during a TLS 1.3 resumption handshake. A DHE key exchange ensures forward secrecy even in the event that ticket keys are compromised, at the expense of an additional round trip and resources required to carry out the DHE key exchange. If disabled, a DHE key exchange will be performed when a PSK is accepted but only if requested by the client. If enabled, the server will require a DHE key exchange when a PSK is accepted regardless of whether the client supports combined PSK-DHE key exchange. This setting only has an effect when

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			resumption is enabled. Default value: NO Possible values = YES, NO
defaultsni	<String>	Read-write	Default domain name supported by the SSL virtual server. The parameter is effective, when zero touch certificate management is active for the SSL virtual server i.e. no manual SNI cert or default server cert is bound to the v-server. For SSL transactions, when SNI is not presented by the client, server-certificate corresponding to the default SNI, if available in the cert-store, is selected else connection is terminated. Minimum length = 1 Maximum length = 126

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
sslclientlogs	<String>	Read-write	This parameter is used to enable or disable the logging of additional information, such as the Session ID and SNI names, from SSL handshakes to the audit logs. Default value: DISABLED Possible values = ENABLED, DISABLED
strictclientekucheck	<String>	Read-write	Enable strict EKU extension check during client authentication. Default value: ENABLED Possible values = ENABLED, DISABLED
crlcheck	<String>	Read-only	The state of the CRL check parameter. (Mandatory/ Optional). Possible values = Mandatory, Optional
nonfipsciphers	<String>	Read-only	The state of usage of non FIPS approved ciphers.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: DISABLED Possible values = ENABLED, DISABLED
service	<Integer>	Read-only	Service. Minimum value = 0 Maximum value = 65534
ocspcheck	<String>	Read-only	The state of the OCSP check parameter. (Mandatory/ Optional). Possible values = Mandatory, Optional
ca	<Boolean>	Read-only	CA certificate.
snicert	<Boolean>	Read-only	The name of the CertKey. Use this option to bind Certkey(s) which will be used in SNI processing.
skipcaname	<Boolean>	Read-only	The flag is used to indicate whether this particular CA certificate's CA_Name needs to be sent to the SSL client while requesting for client certificate in a SSL handshake.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
dtlsflag	<Boolean>	Read-only	The flag is used to indicate whether DTLS is set or not.
quicflag	<Boolean>	Read-only	This flag is used to indicate the use of the QUIC transport protocol by an SSL virtual server or service.
skipcacertbundle	<Boolean>	Read-only	The flag is used to indicate whether this particular CA certificate's CA_Name needs to be sent to the SSL client while requesting for client certificate in a SSL handshake.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslvserver **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"sslvserver":{

<b>"vservername":<String_value>,

</b>"cleartextport":<Integer_value>,

"dh":<String_value>,
```

```
"dhfile":<String_value>,

"dhcount":<Integer_value>,

"dhkeyexpsizelimit":<String_value>,

"ersa":<String_value>,

"ersacount":<Integer_value>,

"sessreuse":<String_value>,

"sesstimeout":<Integer_value>,

"cipherredirect":<String_value>,

"cipherurl":<String_value>,

"sslv2redirect":<String_value>,

"sslv2url":<String_value>,

"clientauth":<String_value>,

"clientcert":<String_value>,

"sslredirect":<String_value>,

"redirectportrewrite":<String_value>,

"ssl2":<String_value>,

"ssl3":<String_value>,

"tls1":<String_value>,

"tls11":<String_value>,

"tls12":<String_value>,

"tls13":<String_value>,

"dtls1":<String_value>,
```

```
"dtls12":<String_value>,

"snienable":<String_value>,

"ocspstapling":<String_value>,

"pushenctrigger":<String_value>,

"sendclosenotify":<String_value>,

"dtlsprofilename":<String_value>,

"sslprofile":<String_value>,

"hsts":<String_value>,

"maxage":<Integer_value>,

"includesubdomains":<String_value>,

"preload":<String_value>,

"strictsigdigestcheck":<String_value>,

"zerorttearlydata":<String_value>,

"tls13sessionticketsperauthcontext":<Integer_value>,

"dhekeyexchangewithpsk":<String_value>,

"defaultsni":<String_value>,

"sslclientlogs":<String_value>,

"strictclientekucheck":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslvserver? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"sslvserver":{

<b>"vservername":<String_value>,

</b>"cleartextport":true,

"dh":true,

"dhfile":true,

"dhcount":true,

"dhkeyexpsizelimit":true,

"ersa":true,

"ersacount":true,

"sessreuse":true,

"sesstimeout":true,

"cipherredirect":true,

"cipherurl":true,

"sslv2redirect":true,
```

```
"sslv2url":true,

"clientauth":true,

"clientcert":true,

"sslredirect":true,

"redirectportrewrite":true,

"ssl2":true,

"ssl3":true,

"tls1":true,

"tls11":true,

"tls12":true,

"tls13":true,

"dtls1":true,

"dtls12":true,

"snienable":true,

"ocspstapling":true,

"sendclosenotify":true,

"dtlsprofilename":true,

"sslprofile":true,

"hsts":true,

"maxage":true,

"includesubdomains":true,

"preload":true,
```

```
"strictsigdigestcheck":true,

"zerorttearlydata":true,

"tls13sessionticketsperauthcontext":true,

"dhekeyexchangewithpsk":true,

"defaultsni":true,

"sslclientlogs":true,

"strictclientekucheck":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslvserver **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/sslvserver? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/sslvserver? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of sslvserver resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/sslvserver? **view=summary**

Use this query-parameter to get the summary output of sslvserver resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/sslvserver? **pagesize=#no;pageno=#no**

Use this query-parameter to get the sslvserver resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "sslvserver": [ {

"vservername":<String_value>,

"cleartextport":<Integer_value>,

"dh":<String_value>,

"dhfile":<String_value>,

"dhcount":<Integer_value>,

"dhkeyexpsizelimit":<String_value>,

"ersa":<String_value>,

"ersacount":<Integer_value>,

"sessreuse":<String_value>,

"sesstimeout":<Integer_value>,

"cipherredirect":<String_value>,
```

```
"crlcheck":<String_value>,

"cipherurl":<String_value>,

"sslv2redirect":<String_value>,

"sslv2url":<String_value>,

"clientauth":<String_value>,

"clientcert":<String_value>,

"sslredirect":<String_value>,

"redirectportrewrite":<String_value>,

"nonfipsciphers":<String_value>,

"ssl2":<String_value>,

"ssl3":<String_value>,

"tls1":<String_value>,

"tls11":<String_value>,

"tls12":<String_value>,

"tls13":<String_value>,

"dtls1":<String_value>,

"dtls12":<String_value>,

"snienable":<String_value>,

"ocspstapling":<String_value>,

"service":<Integer_value>,

"servicename":<String_value>,

"ocspcheck":<String_value>,
```

```
"pushenctrigger":<String_value>,

"ca":<Boolean_value>,

"snicert":<Boolean_value>,

"skipcaname":<Boolean_value>,

"sendclosenotify":<String_value>,

"dtlsprofilename":<String_value>,

"dtlsflag":<Boolean_value>,

"quicflag":<Boolean_value>,

"sslprofile":<String_value>,

"hsts":<String_value>,

"maxage":<Integer_value>,

"includesubdomains":<String_value>,

"preload":<String_value>,

"strictsigdigestcheck":<String_value>,

"zerorttearlydata":<String_value>,

"tls13sessionticketsperauthcontext":<Integer_value>,

"dhekeyexchangewithpsk":<String_value>,

"skipcacertbundle":<Boolean_value>,

"defaultsni":<String_value>,

"sslclientlogs":<String_value>,

"strictclientekucheck":<String_value>,

"_nextgenapiresource":<String_value>
```

```
}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslvserver/ vservername_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/sslvserver/ vservername_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/sslvserver/ vservername_value<String> ? **view=summary**

Use this query-parameter to get the summary output of sslvserver resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslvserver": [ {

"vservername":<String_value>,

"cleartextport":<Integer_value>,
```

```
"dh":<String_value>,

"dhfile":<String_value>,

"dhcount":<Integer_value>,

"dhkeyexpsizelimit":<String_value>,

"ersa":<String_value>,

"ersacount":<Integer_value>,

"sessreuse":<String_value>,

"sesstimeout":<Integer_value>,

"cipherredirect":<String_value>,

"crlcheck":<String_value>,

"cipherurl":<String_value>,

"sslv2redirect":<String_value>,

"sslv2url":<String_value>,

"clientauth":<String_value>,

"clientcert":<String_value>,

"sslredirect":<String_value>,

"redirectportrewrite":<String_value>,

"nonfipsciphers":<String_value>,

"ssl2":<String_value>,

"ssl3":<String_value>,

"tls1":<String_value>,

"tls11":<String_value>,
```

```
"tls12":<String_value>,

"tls13":<String_value>,

"dtls1":<String_value>,

"dtls12":<String_value>,

"snienable":<String_value>,

"ocspstapling":<String_value>,

"service":<Integer_value>,

"servicename":<String_value>,

"ocspcheck":<String_value>,

"pushenctrigger":<String_value>,

"ca":<Boolean_value>,

"snicert":<Boolean_value>,

"skipcaname":<Boolean_value>,

"sendclosenotify":<String_value>,

"dtlsprofilename":<String_value>,

"dtlsflag":<Boolean_value>,

"quicflag":<Boolean_value>,

"sslprofile":<String_value>,

"hsts":<String_value>,

"maxage":<Integer_value>,

"includesubdomains":<String_value>,

"preload":<String_value>,
```

```
"strictsigdigestcheck":<String_value>,

"zerorttearlydata":<String_value>,

"tls13sessionticketsperauthcontext":<Integer_value>,

"dhekeyexchangewithpsk":<String_value>,

"skipcacertbundle":<Boolean_value>,

"defaultsni":<String_value>,

"sslclientlogs":<String_value>,

"strictclientekucheck":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslvserver? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "sslvserver": [ { "__count": "#no"} ] }
```

sslvserver_binding

Binding object which returns the resources bound to sslvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
vservername	<String>	Read-write	Name of the SSL virtual server for which to show detailed information. Minimum length = 1
sslvserver_sslcacertbundle_binding	<sslvserver_sslcacertbundle_binding[]>	Read-only	sslcacertbundle that can be bound to sslvserver.
sslvserver_sslpolicy_binding	<sslvserver_sslpolicy_binding[]>	Read-only	sslpolicy that can be bound to sslvserver.
sslvserver_sslciphersuite_binding	<sslvserver_sslciphersuite_binding[]>	Read-only	sslciphersuite that can be bound to sslvserver.
sslvserver_sslcertkey_binding	<sslvserver_sslcertkey_binding[]>	Read-only	sslcertkey that can be bound to sslvserver.
sslvserver_sslcertkeybundle_binding	<sslvserver_sslcertkeybundle_binding[]>	Read-only	sslcertkeybundle that can be bound to sslvserver.
sslvserver_ecccurve_binding	<sslvserver_ecccurve_binding[]>	Read-only	ecccurve that can be bound to sslvserver.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
sslvserver_hashicorp_binding	<sslvserver_hashicorp_binding[]>	Read-only	hashicorp that can be bound to sslvserver.
sslvserver_sslcipher_binding	<sslvserver_sslcipher_binding[]>	Read-only	sslcipher that can be bound to sslvserver.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslvserver_binding/ vservername_value<String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "sslvserver_binding": [ {

"vservername":<String_value>,

"sslvserver_sslciphersuite_binding":<sslvserver_sslciphersuite_binding[]_value>,

"sslvserver_sslpolicy_binding":<sslvserver_sslpolicy_binding[]_value>,

"sslvserver_ecccurve_binding":<sslvserver_ecccurve_binding[]_value>,

"sslvserver_hashicorp_binding":<sslvserver_hashicorp_binding[]_value>,

"sslvserver_sslcertkey_binding":<sslvserver_sslcertkey_binding[]_value>,

"sslvserver_sslcacertbundle_binding":<sslvserver_sslcacertbundle_binding[]_value>,

"sslvserver_sslcertkeybundle_binding":<sslvserver_sslcertkeybundle_binding[]_value>,

"sslvserver_sslcipher_binding":<sslvserver_sslcipher_binding[]_value>
```

```
}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslvserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/sslvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "sslvserver_binding": [ {

"vservername":<String_value>,

"sslvserver_sslciphersuite_binding":<sslvserver_sslciphersuite_binding[]_value>,

"sslvserver_sslpolicy_binding":<sslvserver_sslpolicy_binding[]_value>,

"sslvserver_ecccurve_binding":<sslvserver_ecccurve_binding[]_value>,

"sslvserver_hashicorp_binding":<sslvserver_hashicorp_binding[]_value>,
```

```
"sslvserver_sslcertkey_binding":<sslvserver_sslcertkey_binding[]_value>,

"sslvserver_sslcacertbundle_binding":<sslvserver_sslcacertbundle_binding[]
_value>,

"sslvserver_sslcertkeybundle_binding":<sslvserver_sslcertkeybundle_binding
[]_value>,

"sslvserver_sslcipher_binding":<sslvserver_sslcipher_binding[]_value>

}]}
```

sslvserver_ecccurve_binding

Binding object showing the ecccurve that can be bound to sslvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ecccurvename	<String>	Read-write	Named ECC curve bound to vserver/ service. Possible values = ALL, P_224, P_256, P_384, P_521, X_25519, X25519_MLKEM768
vservername	<String>	Read-write	Name of the SSL virtual server. Minimum length = 1
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/sslvserver_ecccurve_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"sslvserver_ecccurve_binding":{

<b>"vservername":<String_value>,

</b>"ecccurvename":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslvserver_ecccurve_binding/ vservername_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/ config/sslvserver_ecccurve_binding/ vservername_value<String> ? **args=ecccurvename: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslvserver_ecccurve_binding/ vservername_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/ config/sslvserver_ecccurve_binding/ vservername_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of sslvserver_ecccurve_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/sslvserver_ecccurve_binding/ vservername_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the sslvserver_ecccurve_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslvserver_ecccurve_binding": [ {

"ecccurvename":<String_value>,

"vservername":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslvserver_ecccurve_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ sslvserver_ecccurve_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslvserver_ecccurve_binding": [ {

"ecccurvename":<String_value>,

"vservername":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslvserver_ecccurve_binding/ vservername_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"sslvserver_ecccurve_binding": [ { "__count": "#no"} ] }
```

sslvserver_hashicorp_binding

Binding object showing the hashicorp that can be bound to sslvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
vault	<String>	Read-write	Name of the configured vault where certificate and/or private-key is placed. Minimum length = 1 Maximum length = 127
vservername	<String>	Read-write	Name of the SSL virtual server. Minimum length = 1
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslvserver_hashicorp_binding/ vservername_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/ config/sslvserver_hashicorp_binding/ vservername_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of sslvserver_hashicorp_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/sslvserver_hashicorp_binding/ vservername_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the sslvserver_hashicorp_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslvserver_hashicorp_binding": [ {

"vault":<String_value>,

"vservername":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslvserver_hashicorp_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/sslvserver_hashicorp_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslvserver_hashicorp_binding": [ {

"vault":<String_value>,

"vservername":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslvserver_hashicorp_binding/ vservername_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"sslvserver_hashicorp_binding": [ { "__count": "#no"} ] }
```

sslvserver_sslcacertbundle_binding

Binding object showing the sslcacertbundle that can be bound to sslvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
skipcacertbundle	<Boolean>	Read-write	The flag is used to indicate whether this particular CA certificate's CA_Name needs to be sent to the SSL client while requesting for client certificate in a SSL handshake.
vservername	<String>	Read-write	Name of the SSL virtual server. Minimum length = 1
cacertbundlename	<String>	Read-write	CA certbundle name bound to the vserver. Minimum length = 1 Maximum length = 127
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/sslvserver_sslcacertbundle_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"sslvserver_sslcacertbundle_binding":{
```

```
<b>"vservername":<String_value>,

</b>"cacertbundlename":<String_value>,

"skipcacertbundle":<Boolean_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslvserver_sslcacertbundle_binding/ vservername_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/ config/sslvserver_sslcacertbundle_binding/ vservername_value<String> ? **args=cacertbundlename: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslvserver_sslcacertbundle_binding/ vservername_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/ config/sslvserver_sslcacertbundle_binding/ vservername_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of sslvserver_sslcacertbundle_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/sslvserver_sslcacertbundle_binding/ vservername_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the sslvserver_sslcacertbundle_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslvserver_sslcacertbundle_binding": [ {

"skipcacertbundle":<Boolean_value>,

"vservername":<String_value>,

"cacertbundlename":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslvserver_sslcacertbundle_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/sslvserver_sslcacertbundle_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslvserver_sslcacertbundle_binding": [ {

"skipcacertbundle":<Boolean_value>,

"vservername":<String_value>,

"cacertbundlename":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslvserver_sslcacertbundle_binding/ vservername_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"sslvserver_sslcacertbundle_binding": [ { "__count": "#no"} ] }
```

sslvserver_sslcertkey_binding

Binding object showing the sslcertkey that can be bound to sslvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
snicert	<Boolean>	Read-write	The name of the CertKey. Use this option to bind Certkey(s) which will be used in SNI processing.
crlcheck	<String>	Read-write	The state of the CRL check parameter. (Mandatory/ Optional). Possible values = Mandatory, Optional
ocspcheck	<String>	Read-write	The state of the OCSP check parameter. (Mandatory/ Optional). Possible values = Mandatory, Optional
certkeyname	<String>	Read-write	The name of the certificate key pair binding.
skipcaname	<Boolean>	Read-write	The flag is used to indicate whether this

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			particular CA certificate's CA_Name needs to be sent to the SSL client while requesting for client certificate in a SSL handshake.
vservername	<String>	Read-write	Name of the SSL virtual server. Minimum length = 1
ca	<Boolean>	Read-write	CA certificate.
cleartextport	<Integer>	Read-only	Port on which clear-text data is sent by the appliance to the server. Do not specify this parameter for SSL offloading with end-to-end encryption. Default value: 0 Minimum value = 0 Maximum value = 65534
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)

- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/sslvserver_sslcertkey_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"sslvserver_sslcertkey_binding":{

<b>"vservername":<String_value>,

</b>"certkeyname":<String_value>,

"ca":<Boolean_value>,

"crlcheck":<String_value>,

"skipcaname":<Boolean_value>,

"snicert":<Boolean_value>,

"ocspcheck":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslvserver_sslcertkey_binding/ vservername_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/ config/sslvserver_sslcertkey_binding/ vservername_value<String> ? **args=certkeyname: <String_value> ,ca: <Boolean_value> ,crlcheck: <String_value> ,snicert: <Boolean_value> ,ocspcheck: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslvserver_sslcertkey_binding/ vservername_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/ config/sslvserver_sslcertkey_binding/ vservername_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of sslvserver_sslcertkey_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/sslvserver_sslcertkey_binding/ vservername_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the sslvserver_sslcertkey_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslvserver_sslcertkey_binding": [ {

"snicert":<Boolean_value>,

"crlcheck":<String_value>,

"ocspcheck":<String_value>,

"certkeyname":<String_value>,

"skipcaname":<Boolean_value>,
```

```
"vservername":<String_value>,

"ca":<Boolean_value>,

"cleartextport":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslvserver_sslcertkey_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/sslvserver_sslcertkey_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslvserver_sslcertkey_binding": [ {

"snicert":<Boolean_value>,

"crlcheck":<String_value>,
```

```
"ocspcheck":<String_value>,

"certkeyname":<String_value>,

"skipcaname":<Boolean_value>,

"vservername":<String_value>,

"ca":<Boolean_value>,

"cleartextport":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslvserver_sslcertkey_binding/ vservername_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"sslvserver_sslcertkey_binding": [ { "__count": "#no"} ] }
```

sslvserver_sslcertkeybundle_binding

Binding object showing the sslcertkeybundle that can be bound to sslvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
certkeybundlename	<String>	Read-write	Certkeybundle name bound to the vserver.
vservername	<String>	Read-write	Name of the SSL virtual server. Minimum length = 1
snicertkeybundle	<Boolean>	Read-write	Use this option to bind certkeybundle which will be used in SNI processing.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/sslvserver_sslcertkeybundle_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"sslvserver_sslcertkeybundle_binding":{

<b>"vservername":<String_value>,

</b>"certkeybundlename":<String_value>,

"snicertkeybundle":<Boolean_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslvserver_sslcertkeybundle_binding/ vservername_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/ config/sslvserver_sslcertkeybundle_binding/ vservername_value<String> ? **args=certkeybundlename: <String_value> ,snicertkeybundle: <Boolean_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslvserver_sslcertkeybundle_binding/ vservername_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/ config/sslvserver_sslcertkeybundle_binding/ vservername_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of sslvserver_sslcertkeybundle_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/sslvserver_sslcertkeybundle_binding/ vservername_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the sslvserver_sslcertkeybundle_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslvserver_sslcertkeybundle_binding": [ {

"certkeybundlename":<String_value>,

"vservername":<String_value>,

"snicertkeybundle":<Boolean_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslvserver_sslcertkeybundle_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/sslvserver_sslcertkeybundle_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslvserver_sslcertkeybundle_binding": [ {

"certkeybundlename":<String_value>,

"vservername":<String_value>,

"snicertkeybundle":<Boolean_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslvserver_sslcertkeybundle_binding/ vservername_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"sslvserver_sslcertkeybundle_binding": [ { "__count": "#no"} ] }
```

sslvserver_sslcipher_binding

Binding object showing the sslcipher that can be bound to sslvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
description	<String>	Read-write	The cipher suite description.
vservername	<String>	Read-write	Name of the SSL virtual server. Minimum length = 1
cipheraliasname	<String>	Read-write	The name of the cipher group/alias/ individual cipheri bindings.
ciphername	<String>	Read-write	Name of the individual cipher, user-defined cipher group, or predefined (built-in) cipher alias.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/sslvserver_sslcipher_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"sslvserver_sslcipher_binding":{

<b>"vservername":<String_value>,

</b>"ciphername":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslvserver_sslcipher_binding/ vservername_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/ config/sslvserver_sslcipher_binding/ vservername_value<String> ? **args=ciphername: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslvserver_sslcipher_binding/ vservername_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/ config/sslvserver_sslcipher_binding/ vservername_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of sslvserver_sslcipher_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/sslvserver_sslcipher_binding/ vservername_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the sslvserver_sslcipher_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslvserver_sslcipher_binding": [ {

"description":<String_value>,

"vservername":<String_value>,

"cipheraliasname":<String_value>,

"ciphername":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslvserver_sslcipher_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/sslvserver_sslcipher_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslvserver_sslcipher_binding": [ {

"description":<String_value>,

"vservername":<String_value>,

"cipheraliasname":<String_value>,

"ciphername":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslvserver_sslcipher_binding/ vservername_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"sslvserver_sslcipher_binding": [ { "__count": "#no"} ] }
```

sslvserver_sslciphersuite_binding

Binding object showing the sslciphersuite that can be bound to sslvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
description	<String>	Read-write	The cipher suite description.
vservername	<String>	Read-write	Name of the SSL virtual server. Minimum length = 1
ciphername	<String>	Read-write	The cipher group/ alias/individual cipher configuration.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/sslvserver_sslciphersuite_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"sslvserver_sslciphersuite_binding":{

<b>"vservername":<String_value>,

</b>"ciphername":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslvserver_sslciphersuite_binding/ vservername_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/ config/sslvserver_sslciphersuite_binding/ vservername_value<String> ? **args=ciphername: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslvserver_sslciphersuite_binding/ vservername_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/ config/sslvserver_sslciphersuite_binding/ vservername_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of sslvserver_sslciphersuite_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/sslvserver_sslciphersuite_binding/ vservername_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the sslvserver_sslciphersuite_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslvserver_sslciphersuite_binding": [ {

"description":<String_value>,

"vservername":<String_value>,

"ciphername":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslvserver_sslciphersuite_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/sslvserver_sslciphersuite_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslvserver_sslciphersuite_binding": [ {

"description":<String_value>,

"vservername":<String_value>,

"ciphername":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslvserver_sslciphersuite_binding/ vservername_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"sslvserver_sslciphersuite_binding": [ { "__count": "#no"} ] }
```

sslvserver_sslpolicy_binding

Binding object showing the sslpolicy that can be bound to sslvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
labelname	<String>	Read-write	Name of the label to invoke if the current policy rule evaluates to TRUE.
labeltype	<String>	Read-write	Type of policy label invocation. Possible values = vserver, service, policylabel
priority	<Integer>	Read-write	The priority of the policies bound to this SSL service. Minimum value = 0 Maximum value = 65534
policyname	<String>	Read-write	The name of the SSL policy binding.
gotopriorityexpression	<String>	Read-write	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
invoke	<Boolean>	Read-write	Invoke flag. This attribute is relevant only for ADVANCED policies.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
vservername	<String>	Read-write	Name of the SSL virtual server. Minimum length = 1
type	<String>	Read-write	Bind point to which to bind the policy. Possible Values: REQUEST, INTERCEPT_REQ, CLIENTHELLO_REQ and CLIENT_AUTH_VAL_REQ. These bindpoints mean: 1. REQUEST: Policy evaluation will be done at appplication above SSL. This bindpoint is default and is used for actions based on clientauth and client cert. 2. INTERCEPT_REQ: Policy evaluation will be done during SSL handshake to decide whether to intercept or not. Actions allowed with this type are: INTERCEPT, BYPASS and RESET. 3. CLIENTHELLO_REQ: Policy evaluation will be done during handling of Client Hello Request. Action allowed with this type is: RESET, FORWARD,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			PICKCACERTGRP and OCSPSTAPLING. 4. CLIENT_AUTH_VAL_REQ: Policy evaluation will be performed during the verification of the client certificate. Action allowed with this type is: OCSPCERTVALIDATION. Default value: REQUEST Possible values = INTERCEPT_REQ, REQUEST, CLIENTHELLO_REQ, CLIENT_AUTH_VAL
polinherit	<Integer>	Read-only	Whether the bound policy is a inherited policy or not. Minimum value = 0 Maximum value = 254
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/sslvserver_sslpolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"sslvserver_sslpolicy_binding":{

<b>"vservername":<String_value>,

</b>"policyname":<String_value>,

"priority":<Integer_value>,

"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>,

"labeltype":<String_value>,

"labelname":<String_value>,

"type":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslvserver_sslpolicy_binding/ vservername_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/ config/sslvserver_sslpolicy_binding/ vservername_value<String> ? **args=policyname: <String_value> ,priority: <Integer_value> ,type: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslvserver_sslpolicy_binding/ vservername_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/ config/sslvserver_sslpolicy_binding/ vservername_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of sslvserver_sslpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/sslvserver_sslpolicy_binding/ vservername_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the sslvserver_sslpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslvserver_sslpolicy_binding": [ {

"labelname":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,
```

```
"policyname":<String_value>,

"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>,

"vservername":<String_value>,

"type":<String_value>,

"polinherit":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslvserver_sslpolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/sslvserver_sslpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslvserver_sslpolicy_binding": [ {

"labelname":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"policyname":<String_value>,

"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>,

"vservername":<String_value>,

"type":<String_value>,

"polinherit":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslvserver_sslpolicy_binding/ vservername_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"sslvserver_sslpolicy_binding": [ { "__count": "#no"} ] }
```

sslwrapkey

Configuration for WRAP key resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
wrapkeyname	<String>	Read-write	Name for the wrap key. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the wrap key is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			"my key" or 'my key'). Minimum length = 1
password	<String>	Read-write	Password string for the wrap key. Minimum length = 1
salt	<String>	Read-write	Salt string for the wrap key. Minimum length = 1
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- CREATE
- DELETE
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of

creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

CREATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslwrapkey? **action=create HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"sslwrapkey":{

<b>"wrapkeyname":<String_value>,

</b><b>"password":<String_value>,

</b><b>"salt":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslwrapkey/ wrapkeyname_value<String>
HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslwrapkey **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/sslwrapkey? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/sslwrapkey? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of sslwrapkey resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/sslwrapkey? **view=summary**

Use this query-parameter to get the summary output of sslwrapkey resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/sslwrapkey? **pagesize=#no;pageno=#no**

Use this query-parameter to get the sslwrapkey resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "sslwrapkey": [ {

"wrapkeyname":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslwrapkey? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "sslwrapkey": [ { "__count": "#no"} ] }
```

stream

Stream

Stream configuration.

NAME	DESCRIPTION
streamidentifier	Configuration for identifier
streamidentifier_analyticsprofile_binding	Binding object showing the analyticsprofile that can be bound to streamidentifier
streamidentifier_binding	Binding object showing the resources that can be bound to streamidentifier
streamidentifier_streamsession_binding	Binding object showing the streamsession that can be bound to streamidentifier
streamselector	Configuration for selector
streamsession	Configuration for active connection

streamidentifier

Configuration for identifier resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	The name of stream identifier.
selectorname	<String>	Read-write	Name of the selector to use with the stream identifier.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum length = 1
interval	<Integer>	Read-write	Number of minutes of data to use when calculating session statistics (number of requests, bandwidth, and response times). The interval is a moving window that keeps the most recently collected data. Older data is discarded at regular intervals. Default value: 1 Minimum value = 1 Maximum value = 10080
samplecount	<Integer>	Read-write	Size of the sample from which to select a request for evaluation. The smaller the sample count, the more accurate is the statistical data. To evaluate all requests, set the sample count to 1. However, such a low setting can result in excessive consumption of memory and processing resources. Default value: 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum value = 1 Maximum value = 65535
sort	<String>	Read-write	Sort stored records by the specified statistics column, in descending order. Performed during data collection, the sorting enables real-time data evaluation through Citrix ADC policies (for example, compression and caching policies) that use functions such as IS_TOP(n). Default value: REQUESTS Possible values = REQUESTS, CONNECTIONS, RESPTIME, BANDWIDTH, RESPTIME_BREACHES, TOKENS, NONE
snmptrap	<String>	Read-write	Enable/disable SNMP trap for stream identifier. Default value: DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ENABLED, DISABLED
appflowlog	<String>	Read-write	Enable/disable Appflow logging for stream identifier. Default value: DISABLED Possible values = ENABLED, DISABLED
trackackonlypackets	<String>	Read-write	Track ack only packets as well. This setting is applicable only when packet rate limiting is being used. Default value: DISABLED Possible values = ENABLED, DISABLED
tracktransactions	<String>	Read-write	Track transactions exceeding configured threshold. Transaction tracking can be enabled for following metrics: ResponseTime (RESPTIME) or LLM token consumption (TOKENS). When set to TOKENS, minTransactionThre

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			shold, maxTransactionThreshold, acceptanceThreshold and breachThreshold are not applicable. By default transaction tracking is disabled. Default value: NONE Possible values = RESPTIME, TOKENS, NONE
maxtransactionthreshold	<Integer>	Read-write	Maximum per transcation value of metric. Metric to be tracked is specified by tracktransactions attribute. Default value: 0
mintransactionthreshold	<Integer>	Read-write	Minimum per transcation value of metric. Metric to be tracked is specified by tracktransactions attribute. Default value: 0
acceptancethreshold	<String>	Read-write	Non-Breaching transactions to Total transactions

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			threshold expressed in percent. Maximum of 6 decimal places is supported. Default value: 0.000000 Maximum length = 10
breachthreshold	<Integer>	Read-write	Breaching transactions threshold calculated over interval. Default value: 0
log	<String>	Read-write	Location where objects collected on the identifier will be logged. Default value: NONE Possible values = SYSLOG, NONE
loginterval	<Integer>	Read-write	Time interval in minutes for logging the collected objects. Log interval should be greater than or equal to the inteval of the stream identifier. Default value: 5

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum value = 1 Maximum value = 10080
loglimit	<Integer>	Read-write	Maximum number of objects to be logged in the log interval. Default value: 100 Minimum value = 1 Maximum value = 1000
rule	<String[]>	Read-only	Rule.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- UPDATE
- UNSET
- DELETE
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/streamidentifier **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"streamidentifier":{

<b>"name":<String_value>,

</b><b>"selectorname":<String_value>,

</b>"interval":<Integer_value>,

"samplecount":<Integer_value>,

"sort":<String_value>,

"snmptrap":<String_value>,
```

```
"appflowlog":<String_value>,

"trackackonlypackets":<String_value>,

"tracktransactions":<String_value>,

"maxtransactionthreshold":<Integer_value>,

"mintransactionthreshold":<Integer_value>,

"acceptancethreshold":<String_value>,

"breachthreshold":<Integer_value>,

"log":<String_value>,

"loginterval":<Integer_value>,

"loglimit":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/streamidentifier **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"streamidentifier":{

<b>"name":<String_value>,
```

```
</b>"selectorname":<String_value>,

"interval":<Integer_value>,

"samplecount":<Integer_value>,

"sort":<String_value>,

"snmptrap":<String_value>,

"appflowlog":<String_value>,

"trackackonlypackets":<String_value>,

"tracktransactions":<String_value>,

"maxtransactionthreshold":<Integer_value>,

"mintransactionthreshold":<Integer_value>,

"acceptancethreshold":<String_value>,

"breachthreshold":<Integer_value>,

"log":<String_value>,

"loginterval":<Integer_value>,

"loglimit":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/streamidentifier? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"streamidentifier":{

<b>"name":<String_value>,

</b>"selectorname":true,

"interval":true,

"samplecount":true,

"sort":true,

"snmptrap":true,

"appflowlog":true,

"trackackonlypackets":true,

"tracktransactions":true,

"maxtransactionthreshold":true,

"mintransactionthreshold":true,

"acceptancethreshold":true,

"breachthreshold":true,

"log":true,

"loginterval":true,

"loglimit":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/streamidentifier/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/streamidentifier **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/streamidentifier? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/streamidentifier? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of streamidentifier resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/streamidentifier? **view=summary**

Use this query-parameter to get the summary output of streamidentifier resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/streamidentifier? **pagesize=#no;pageno=#no**

Use this query-parameter to get the streamidentifier resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "streamidentifier": [ {

"name":<String_value>,

"selectorname":<String_value>,

"rule":<String[]_value>,

"interval":<Integer_value>,

"samplecount":<Integer_value>,

"sort":<String_value>,

"snmptrap":<String_value>,

"appflowlog":<String_value>,

"trackackonlypackets":<String_value>,

"tracktransactions":<String_value>,

"maxtransactionthreshold":<Integer_value>,

"mintransactionthreshold":<Integer_value>,
```

```
"acceptancethreshold":<String_value>,

"breachthreshold":<Integer_value>,

"log":<String_value>,

"loginterval":<Integer_value>,

"loglimit":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/streamidentifier/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/streamidentifier/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/streamidentifier/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of streamidentifier resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "streamidentifier": [ {

"name":<String_value>,

"selectorname":<String_value>,

"rule":<String[]_value>,

"interval":<Integer_value>,

"samplecount":<Integer_value>,

"sort":<String_value>,

"snmptrap":<String_value>,

"appflowlog":<String_value>,

"trackackonlypackets":<String_value>,

"tracktransactions":<String_value>,

"maxtransactionthreshold":<Integer_value>,

"mintransactionthreshold":<Integer_value>,

"acceptancethreshold":<String_value>,

"breachthreshold":<Integer_value>,

"log":<String_value>,

"loginterval":<Integer_value>,

"loglimit":<Integer_value>,

"_nextgenapiresource":<String_value>
```

```
}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/streamidentifier? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "streamidentifier": [ { "__count": "#no"} ] }
```

streamidentifier_analyticsprofile_binding

Binding object showing the analyticsprofile that can be bound to streamidentifier.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
analyticsprofile	<String>	Read-write	Name of the analytics profile.
name	<String>	Read-write	The name of stream identifier.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/streamidentifier_analyticsprofile_binding

HTTP Method: PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"streamidentifier_analyticsprofile_binding":{

<b>"name":<String_value>,

</b>"analyticsprofile":<String_value>

}}
```

Response:

HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/streamidentifier_analyticsprofile_binding

Query-parameters:

args

http:// <netscaler-ip-address> /nitro/v1/config/streamidentifier_analyticsprofile_binding? **args= name:<String_value>, analyticsprofile: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/streamidentifier_analyticsprofile_binding

Query-parameters:

filter

http:// <netscaler-ip-address> /nitro/v1/config/streamidentifier_analyticsprofile_binding?**filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of streamidentifier_analyticsprofile_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination

http:// <netscaler-ip-address> /nitro/v1/config/streamidentifier_analyticsprofile_binding?**pagesize=#no;pageno=#no**

Use this query-parameter to get the streamidentifier_analyticsprofile_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "streamidentifier_analyticsprofile_binding": [ {

"analyticsprofile":<String_value>,

"name":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/streamidentifier_analyticsprofile_binding

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters:

bulkbindings

http:// <netscaler-ip-address> /nitro/v1/config/streamidentifier_analyticsprofile_binding?**bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "streamidentifier_analyticsprofile_binding": [ {

"analyticsprofile":<String_value>,

"name":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/streamidentifier_analyticsprofile_binding?**args=;count=yes**

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "streamidentifier_analyticsprofile_binding": [ { "__count": "#no"} ] }
```

streamidentifier_binding

Binding object which returns the resources bound to streamidentifier.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	The name of stream identifier.
streamidentifier_streamsession_binding	<streamidentifier_streamsession_binding[]>	Read-only	streamsession that can be bound to streamidentifier.
streamidentifier_analyticsprofile_binding	<streamidentifier_analyticsprofile_binding []>	Read-only	analyticsprofile that can be bound to streamidentifier.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/streamidentifier_binding/ name_value<String>

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "streamidentifier_binding": [ {

"name":<String_value>,
```

```
"streamidentifier_analyticsprofile_binding":<streamidentifier_analyticspro
file_binding[]_value>,

"streamidentifier_streamsession_binding":<streamidentifier_streamsession_b
inding[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/streamidentifier_binding

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters:

bulkbindings

http:// <netscaler-ip-address> /nitro/v1/config/streamidentifier_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "streamidentifier_binding": [ {

"name":<String_value>,

"streamidentifier_analyticsprofile_binding":<streamidentifier_analyticspro
file_binding[]_value>,

"streamidentifier_streamsession_binding":<streamidentifier_streamsession_b
inding[]_value>

}]}
```

streamidentifier_streamsession_binding

Binding object showing the streamsession that can be bound to streamidentifier.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	The name of stream identifier.
analyticsprofile	<String>	Read-write	Name of the analytics profile.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/streamidentifier_streamsession_binding
Query-parameters: filter http:// <netscaler-ip-address> /nitro/v1/config/streamidentifier_streamsession_binding? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of streamidentifier_streamsession_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/streamidentifier_streamsession_binding? **pagesize=#no;pageno=#no**

Use this query-parameter to get the streamidentifier_streamsession_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "streamidentifier_streamsession_binding": [ {

"name":<String_value>,

"analyticsprofile":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/streamidentifier_streamsession_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/streamidentifier_streamsession_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "streamidentifier_streamsession_binding": [ {

"name":<String_value>,

"analyticsprofile":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/streamidentifier_streamsession_binding?**args=;count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "streamidentifier_streamsession_binding": [ { "__count": "#no"} ] }
```

streamselector

Configuration for selector resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the selector. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. If the name includes one or more spaces, and you are using the Citrix ADC CLI, enclose the name in double or single quotation marks (for example, "my selector" or 'my selector').
rule	<String[]>	Read-write	Set of up to five expressions. Maximum length: 7499 characters. Each expression must identify a specific request characteristic, such as the client's IP

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			address (with CLIENT.IP.SRC) or requested server resource (with HTTP.REQ.URL). Note: If two or more selectors contain the same expressions in different order, a separate set of records is created for each selector. Minimum length = 1
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- UPDATE
- DELETE
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/streamselector **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"streamselector":{

<b>"name":<String_value>,

</b><b>"rule":<String[]_value>

</b>}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/streamselector **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"streamselector":{

<b>"name":<String_value>,

</b>"rule":<String[]_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/streamselector/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/streamselector **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/streamselector? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/streamselector? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of streamselector resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/streamselector? **view=summary**

Use this query-parameter to get the summary output of streamselector resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/streamselector? **pagesize=#no;pageno=#no**

Use this query-parameter to get the streamselector resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "streamselector": [ {

"name":<String_value>,

"rule":<String[]_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/streamselector/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/streamselector/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/streamselector/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of streamselector resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "streamselector": [ {

"name":<String_value>,

"rule":<String[]_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/streamselector? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "streamselector": [ { "__count": "#no"} ] }
```

streamsession

Configuration for active connection resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the stream identifier. Minimum length = 1

Operations

(click to see Properties)

- CLEAR

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

CLEAR

URL: http:// <netscaler-ip-address> /nitro/v1/config/streamsession? **action=clear HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"streamsession":{

<b>"name":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

subscriber

Subscriber

Subscriber configuration

NAME	DESCRIPTION
subscribergxinterface	Configuration for Gx interface Parameters
subscriberparam	Configuration for Subscriber Params
subscriberprofile	Configuration for Subscriber Profile
subscriberradiusinterface	Configuration for RADIUS interface Parameters
subscribersessions	Configuration for subscriber sesions

subscribergxinterface

Configuration for Gx interface Parameters resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
vserver	<String>	Read-write	Name of the load balancing, or content switching vserver to which the Gx connections are established. The service type of the virtual server must be DIAMETER/ SSL_DIAMETER. Mutually exclusive with the service parameter. Therefore, you cannot set both service and the Virtual Server in the Gx Interface. Minimum length = 1
service	<String>	Read-write	Name of DIAMETER/ SSL_DIAMETER service corresponding to PCRF to which the Gx connection is established. The service type of the service must be DIAMETER/ SSL_DIAMETER. Mutually exclusive with vserver

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			parameter. Therefore, you cannot set both Service and the Virtual Server in the Gx Interface. Minimum length = 1
pcrfrealm	<String>	Read-write	PCRF realm is of type DiameterIdentity and contains the realm of PCRF to which the message is to be routed. This is the realm used in Destination-Realm AVP by Citrix ADC Gx client (as a Diameter node). Minimum length = 1
holdonsubscriberabsence	<String>	Read-write	Set this setting to yes if Citrix ADC needs to Hold pakcets till subscriber session is fetched from PCRF. Else set to NO. By default set to yes. If this setting is set to NO, then till Citrix ADC fetches subscriber from PCRF, default subscriber profile will be applied to this subscriber if configured. If default subscriber profile is also not configured an undef would be

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			raised to expressions which use Subscriber attributes. . Default value: YES Possible values = YES, NO
requesttimeout	<Integer>	Read-write	q!Time, in seconds, within which the Gx CCR request must complete. If the request does not complete within this time, the request is retransmitted for requestRetryAttempts time. If still reuqest is not complete then default subscriber profile will be applied to this subscriber if configured. If default subscriber profile is also not configured an undef would be raised to expressions which use Subscriber attributes. Zero disables the timeout. !. Default value: 10 Minimum value = 0 Maximum value = 86400

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
requestretryattempts	<Integer>	Read-write	If the request does not complete within requestTimeout time, the request is retransmitted for requestRetryAttempts time. Default value: 3
idlettl	<Integer>	Read-write	q!Idle Time, in seconds, after which the Gx CCR-U request will be sent after any PCRF activity on a session. Any RAR or CCA message resets the timer. Zero value disables the idle timeout. !. Default value: 900 Minimum value = 0 Maximum value = 86400
revalidationtimeout	<Integer>	Read-write	q!Revalidation Timeout, in seconds, after which the Gx CCR-U request will be sent after any PCRF activity on a session. Any RAR or CCA message resets the timer. Zero value disables the idle timeout. !.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: 0 Minimum value = 0 Maximum value = 86400
healthcheck	<String>	Read-write	q!Set this setting to yes if Citrix ADC should send DWR packets to PCRF server. When the session is idle, healthcheck timer expires and DWR packets are initiated in order to check that PCRF server is active. By default set to No. !. Default value: NO Possible values = YES, NO
healthcheckttl	<Integer>	Read-write	q!Healthcheck timeout, in seconds, after which the DWR will be sent in order to ensure the state of the PCRF server. Any CCR, CCA, RAR or RRA message resets the timer. !. Default value: 30 Minimum value = 6 Maximum value = 86400

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
cerrequesttimeout	<Integer>	Read-write	q!Healthcheck request timeout, in seconds, after which the Citrix ADC considers that no CCA packet received to the initiated CCR. After this time Citrix ADC should send again CCR to PCRF server. !. Default value: 0 Minimum value = 0 Maximum value = 86400
negativettl	<Integer>	Read-write	q!Negative TTL, in seconds, after which the Gx CCR-I request will be resent for sessions that have not been resolved by PCRF due to server being down or no response or failed response. Instead of polling the PCRF server constantly, negative-TTL makes Citrix ADC stick to un-resolved session. Meanwhile Citrix ADC installs a negative session to avoid going to PCRF.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			For Negative Sessions, Netcaler inherits the attributes from default subscriber profile if default subscriber is configured. A default subscriber could be configured as 'add subscriber profile *'. Or these attributes can be inherited from Radius as well if Radius is configued. Zero value disables the Negative Sessions. And Citrix ADC does not install Negative sessions even if subscriber session could not be fetched. !. Default value: 600 Minimum value = 0 Maximum value = 86400
negativettllimitedsuccess	<String>	Read-write	Set this to YES if Citrix ADC should create negative session for Result-

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Code DIAMETER_LIMITED_SUCCESS (2002) received in CCA-I. If set to NO, regular session is created. Default value: NO Possible values = YES, NO
purgesdbongxfailure	<String>	Read-write	Set this setting to YES if needed to purge Subscriber Database in case of Gx failure. By default set to NO. . Default value: NO Possible values = YES, NO
servicepathavp	<Integer[]>	Read-write	The AVP code in which PCRF sends service path applicable for subscriber. Minimum value = 1
servicepathvendorid	<Integer>	Read-write	The vendorid of the AVP in which PCRF sends service path for subscriber.
nodeid	<Integer>	Read-write	Unique number that identifies the cluster node. Minimum value = 0 Maximum value = 31

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
svrstate	<String>	Read-only	The state of the gx service. Possible values = UP, DOWN, UNKNOWN, BUSY, OUT OF SERVICE, GOING OUT OF SERVICE, DOWN WHEN GOING OUT OF SERVICE, NS_EMPTY_STR, Unknown, DISABLED
identity	<String>	Read-only	DiameterIdentity to be used by NS. DiameterIdentity is used to identify a Diameter node uniquely. Before setting up diameter configuration, Citrix ADC (as a Diameter node) MUST be assigned a unique DiameterIdentity. example => set ns diameter -identity Citrix ADC.com Now whenever Citrix ADC system needs to use identity in diameter messages. It will use 'netscaler.com'

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			as Origin-Host AVP as defined in RFC3588 . Minimum length = 1
realm	<String>	Read-only	Diameter Realm to be used by NS. example => set ns diameter -realm com Now whenever Citrix ADC system needs to use realm in diameter messages. It will use 'com' as Origin-Realm AVP as defined in RFC3588 . Minimum length = 1
status	<String>	Read-only	Citrix ADC PCRF connection Status. (Gx Protocol State).
servicepathinfomode	<String>	Read-only	The type of info in which service path is passed from PCRF, SERVICE_FUNCTION: Denotes the service chain is passed as servicefunction

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			names in-order in AVPS with code servicepathAVP SERVICE_PATH: Denotes the service path name is passed in AVPS with code servicepathAVP.q. Default value: SERVICEPATH Possible values = SERVICEFUNCTIONS, SERVICEPATH
gxreportingavp1	<Integer[]>	Read-only	The AVP code to report as 1st custom AVP. Minimum value = 1
gxreportingavp1vendorid	<Integer>	Read-only	The vendorid of the AVP which will be reported as 1st custom AVP.
gxreportingavp1type	<String>	Read-only	The type of the AVP which will be reported as 1st custom AVP. Default value: OctetString Possible values = OctetString, Integer32, Integer64, Unsigned32,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Unsigned64, Float32, Float64
gxreportingavp2	<Integer[]>	Read-only	The AVP code to report as 2nd custom AVP. Minimum value = 1
gxreportingavp2vendorid	<Integer>	Read-only	The vendorid of the AVP which will be reported as 2nd custom AVP.
gxreportingavp2type	<String>	Read-only	The type of the AVP which will be reported as 2nd custom AVP. Default value: OctetString Possible values = OctetString, Integer32, Integer64, Unsigned32, Unsigned64, Float32, Float64
gxreportingavp3	<Integer[]>	Read-only	The AVP code to report as 3rd custom AVP. Minimum value = 1
gxreportingavp3vendorid	<Integer>	Read-only	The vendorid of the AVP which will be reported as 3rd custom AVP.
gxreportingavp3type	<String>	Read-only	The type of the AVP which will be

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			reported as 3rd custom AVP. Default value: OctetString Possible values = OctetString, Integer32, Integer64, Unsigned32, Unsigned64, Float32, Float64
gxreportingavp4	<Integer[]>	Read-only	The AVP code to report as 4th custom AVP. Minimum value = 1
gxreportingavp4vendorid	<Integer>	Read-only	The vendorid of the AVP which will be reported as 4th custom AVP.
gxreportingavp4type	<String>	Read-only	The type of the AVP which will be reported as 4th custom AVP. Default value: OctetString Possible values = OctetString, Integer32, Integer64, Unsigned32, Unsigned64, Float32, Float64

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
gxreportingavp5	<Integer[]>	Read-only	The AVP code to report as 5th custom AVP. Minimum value = 1
gxreportingavp5vendorid	<Integer>	Read-only	The vendorid of the AVP which will be reported as 5th custom AVP.
gxreportingavp5type	<String>	Read-only	The type of the AVP which will be reported as 5th custom AVP. Default value: OctetString Possible values = OctetString, Integer32, Integer64, Unsigned32, Unsigned64, Float32, Float64
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- UPDATE
- UNSET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/subscribergxinterface **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"subscribergxinterface":{

"vserver":<String_value>,

"service":<String_value>,

"pcrfrealm":<String_value>,
```

```
"holdonsubscriberabsence":<String_value>,

"requesttimeout":<Integer_value>,

"requestretryattempts":<Integer_value>,

"idlettl":<Integer_value>,

"revalidationtimeout":<Integer_value>,

"healthcheck":<String_value>,

"healthcheckttl":<Integer_value>,

"cerrequesttimeout":<Integer_value>,

"negativettl":<Integer_value>,

"negativettllimitedsuccess":<String_value>,

"purgesdbongxfailure":<String_value>,

"servicepathavp":<Integer[]_value>,

"servicepathvendorid":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/subscribergxinterface? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"subscribergxinterface":{

"vserver":true,

"service":true,

"holdonsubscriberabsence":true,

"requesttimeout":true,

"requestretryattempts":true,

"idlettl":true,

"revalidationtimeout":true,

"healthcheck":true,

"healthchecktttl":true,

"cerrequesttimeout":true,

"negativettl":true,

"negativettllimitedsuccess":true,

"purgesdbongxfailure":true,

"servicepathavp":true,

"servicepathvendorid":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/subscribergxinterface **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/subscribergxinterface? **args=nodeid: <Integer_value>**

Use this query-parameter to get subscribergxinterface resources based on additional properties.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "subscribergxinterface": [ {

nodeid:<Integer_value>"vserver":<String_value>,

"service":<String_value>,

"svrstate":<String_value>,

"pcrfrealm":<String_value>,

"holdonsubscriberabsence":<String_value>,

"requesttimeout":<Integer_value>,

"requestretryattempts":<Integer_value>,

"idlettl":<Integer_value>,
```

```
"revalidationtimeout":<Integer_value>,

"healthcheck":<String_value>,

"healthcheckttl":<Integer_value>,

"cerrequesttimeout":<Integer_value>,

"negativettl":<Integer_value>,

"negativettllimitedsuccess":<String_value>,

"purgesdbongxfailure":<String_value>,

"identity":<String_value>,

"realm":<String_value>,

"status":<String_value>,

"servicepathavp":<Integer[]_value>,

"servicepathvendorid":<Integer_value>,

"servicepathinfomode":<String_value>,

"gxreportingavp1":<Integer[]_value>,

"gxreportingavp1vendorid":<Integer_value>,

"gxreportingavp1type":<String_value>,

"gxreportingavp2":<Integer[]_value>,

"gxreportingavp2vendorid":<Integer_value>,

"gxreportingavp2type":<String_value>,

"gxreportingavp3":<Integer[]_value>,

"gxreportingavp3vendorid":<Integer_value>,

"gxreportingavp3type":<String_value>,
```

```
"gxreportingavp4":<Integer[]_value>,

"gxreportingavp4vendorid":<Integer_value>,

"gxreportingavp4type":<String_value>,

"gxreportingavp5":<Integer[]_value>,

"gxreportingavp5vendorid":<Integer_value>,

"gxreportingavp5type":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

subscriberparam

Configuration for Subscriber Params resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
keytype	<String>	Read-write	Type of subscriber key type IP or IPANDVLAN. IPANDVLAN option can be used only when the interfaceType is set to gxOnly. Changing the lookup method should result to the subscriber session database being flushed.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: IP Possible values = IP, IPANDVLAN
interfacetype	<String>	Read-write	Subscriber Interface refers to Citrix ADC interaction with control plane protocols, RADIUS and GX. Types of subscriber interface: NONE, RadiusOnly, RadiusAndGx, GxOnly. NONE: Only static subscribers can be configured. RadiusOnly: GX interface is absent. Subscriber information is obtained through RADIUS Accounting messages. RadiusAndGx: Subscriber ID obtained through RADIUS Accounting is used to query PCRF. Subscriber information is

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			obtained from both RADIUS and PCRF. GxOnly: RADIUS interface is absent. Subscriber information is queried using Subscriber IP or IP+VLAN. Default value: None Possible values = None, RadiusOnly, RadiusAndGx, GxOnly
idlettl	<Integer>	Read-write	q!Idle Timeout, in seconds, after which Citrix ADC will take an idleAction on a subscriber session (refer to 'idleAction' arguement in 'set subscriber param' for more details on idleAction). Any data-plane or control plane activity updates the idleTimeout on subscriber session. idleAction could be to 'just delete the session' or 'delete and CCR-T' (if PCRF is configured) or 'do not delete but send a CCR-U'.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Zero value disables the idle timeout. !. Default value: 0 Minimum value = 0 Maximum value = 172800
idleaction	<String>	Read-write	q!Once idleTTL exprires on a subscriber session, Citrix ADC will take an idle action on that session. idleAction could be chosen from one of these ==> 1. ccrTerminate: (default) send CCR-T to inform PCRF about session termination and delete the session. 2. delete: Just delete the subscriber session without informing PCRF. 3. ccrUpdate: Do not delete the session and instead send a CCR-U to PCRF requesting

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			for an updated session. !. Default value: ccrTerminate Possible values = ccrTerminate, delete, ccrUpdate
ipv6prefixlookuplist	<Integer[]>	Read-write	The ipv6PrefixLookupList should consist of all the ipv6 prefix lengths assigned to the UE's'. Minimum value = 1 Maximum value = 128
builtin	<String[]>	Read-only	. Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL
feature	<String>	Read-only	The feature to be checked while applying this config.
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- UPDATE
- UNSET

- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/subscriberparam **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"subscriberparam":{

"keytype":<String_value>,
```

```
"interfacetype":<String_value>,

"idlettl":<Integer_value>,

"idleaction":<String_value>,

"ipv6prefixlookuplist":<Integer[]_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/subscriberparam? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"subscriberparam":{

"keytype":true,

"interfacetype":true,

"idlettl":true,

"idleaction":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/subscriberparam **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "subscriberparam": [ {

"keytype":<String_value>,

"interfacetype":<String_value>,

"idlettl":<Integer_value>,

"idleaction":<String_value>,

"ipv6prefixlookuplist":<Integer[]_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

subscriberprofile

Configuration for Subscriber Profile resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ip	<String>	Read-write	Subscriber ip address.
vlan	<Integer>	Read-write	The vlan number on which the subscriber is located. Default value: 0 Minimum value = 0 Maximum value = 4096
subscriberrules	<String[]>	Read-write	Rules configured for this subscriber. This is similar to rules received from PCRF for dynamic subscriber sessions.
subscriptionidtype	<String>	Read-write	Subscription-Id type. Possible values = E164, IMSI, SIP_URI, NAI, PRIVATE
subscriptionidvalue	<String>	Read-write	Subscription-Id value.
servicepath	<String>	Read-write	Name of the servicepath to be taken for this subscriber.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
flags	<Integer>	Read-only	Subscriber Session flags.
ttl	<Integer>	Read-only	Subscriber Session TTL.
avpdisplaybuffer	<String>	Read-only	Subscriber Attributes Display.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- UPDATE
- UNSET
- DELETE
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/subscriberprofile **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"subscriberprofile":{

<b>"ip":<String_value>,

</b>"vlan":<Integer_value>,

"subscriberrules":<String[]_value>,

"subscriptionidtype":<String_value>,

"subscriptionidvalue":<String_value>,

"servicepath":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/subscriberprofile **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"subscriberprofile":{

<b>"ip":<String_value>,

</b>"vlan":<Integer_value>,

"subscriberrules":<String[]_value>,

"subscriptionidtype":<String_value>,

"subscriptionidvalue":<String_value>,

"servicepath":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/subscriberprofile? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"subscriberprofile":{

<b>"ip":<String_value>,

</b>"servicepath":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/subscriberprofile/ ip_value<String> **Query-parameters: args=vlan: <Integer_value>**
get (all)
URL: http:// <netscaler-ip-address> /nitro/v1/config/subscriberprofile **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/subscriberprofile? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/subscriberprofile? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of subscriberprofile resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/subscriberprofile? **view=summary**

Use this query-parameter to get the summary output of subscriberprofile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/subscriberprofile? **pagesize=#no;pageno=#no**

Use this query-parameter to get the subscriberprofile resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "subscriberprofile": [ {

"ip":<String_value>,

"vlan":<Integer_value>,

"subscriptionidtype":<String_value>,

"subscriptionidvalue":<String_value>,

"subscriberrules":<String[]_value>,

"flags":<Integer_value>,

"ttl":<Integer_value>,

"avpdisplaybuffer":<String_value>,

"servicepath":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

count

URL: http:// <netscaler-ip-address> /nitro/v1/config/subscriberprofile? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "subscriberprofile": [ { "__count": "#no"} ] }
```

subscriberradiusinterface

Configuration for RADIUS interface Parameters resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
listeningservice	<String>	Read-write	Name of RADIUS LISTENING service that will process RADIUS accounting requests. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
radiusinterimasstart	<String>	Read-write	Treat radius interim message as start radius messages. Default value: DISABLED Possible values = ENABLED, DISABLED
svrstate	<String>	Read-only	The state of the radius service. Possible values = UP, DOWN, UNKNOWN, BUSY, OUT OF SERVICE, GOING OUT OF SERVICE, DOWN WHEN GOING OUT OF SERVICE, NS_EMPTY_STR, Unknown, DISABLED
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- UPDATE
- UNSET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/subscriberradiusinterface **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"subscriberradiusinterface":{

"listeningservice":<String_value>,

"radiusinterimasstart":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/subscriberradiusinterface? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"subscriberradiusinterface":{

"radiusinterimasstart":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/subscriberradiusinterface **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "subscriberradiusinterface": [ {

"listeningservice":<String_value>,

"svrstate":<String_value>,

"radiusinterimasstart":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

subscribersessions

Configuration for subscriber sesions resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ip	<String>	Read-write	Subscriber IP Address. Default value: 0
vlan	<Integer>	Read-write	The vlan number on which the subscriber is located. Default value: 0 Minimum value = 0 Maximum value = 4096
nodeid	<Integer>	Read-write	Unique number that identifies the cluster node.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum value = 0 Maximum value = 31
subscriptionidtype	<String>	Read-only	Subscription-Id type. Possible values = E164, IMSI, SIP_URI, NAI, PRIVATE
subscriptionidvalue	<String>	Read-only	Subscription-Id value.
subscriberrules	<String[]>	Read-only	Rules stored in this session for this subscriber. When PCRF sends Charging-Rule-Name or Charging-Rule-Base-Name AVP for a subscriber, Citrix ADC stores these AVPs in the subscriber session. These Rules can be retreived using 'Subscriber.Rule_Active(<rule name>)' expression. For static subscriber profiles, these rules are configured using '-subscriberRules <list of rules>'.
flags	<Integer>	Read-only	Subscriber Session flags.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ttl	<Integer>	Read-only	Subscriber Session revalidation Timeout remaining. This TTL gets refreshed when a radius or CCA or RAR message is received for this subscriber session. Citrix ADC will send a CCR-U after revalidation timer expires. If subscriber sessions is a negative session, then Citrix ADC will send a CCR-I after TTL expires. Negative Sessions are sessions which have not been resolved by PCRF and instead of polling PCRF continously, Citrix ADC has installed a negative session. If default subscriber is configued, then Negative Sessions inherits default subscriber profile. .
idlettl	<Integer>	Read-only	Subscriber Session Activity Timeout remaining. Citrix ADC will take an

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			idleAction after ttl expires. idleaction could be --> 1. ccrTerminate: (default) send CCR-T to inform PCRF about session termination and delete the session. 2. delete: Just delete the subscriber session without informing PCRF. 3. ccrUpdate: Do not delete the session and instead send a CCR-U to PCRF requesting for an updated session. But if this is a negative session and idleaction is ccrUpdate then Citrix ADC won't take any action. Also on negative sessions ccrTerminate translates to delete.
avpdisplaybuffer	<String>	Read-only	Subscriber Attributes Display.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
servicepath	<String>	Read-only	Name of the servicepath to be taken for this subscriber.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- CLEAR
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

CLEAR

URL: http:// <netscaler-ip-address> /nitro/v1/config/subscribersessions? **action=clear HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"subscribersessions":{

"ip":<String_value>,

"vlan":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/subscribersessions **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/subscribersessions? **args=ip: <String_value> ,vlan: <Integer_value> ,nodeid: <Integer_value>**

Use this query-parameter to get subscribersessions resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/config/subscribersessions? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/subscribersessions? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of subscribersessions resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/subscribersessions? **view=summary**

Use this query-parameter to get the summary output of subscribersessions resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/subscribersessions? **pagesize=#no;pageno=#no**

Use this query-parameter to get the subscribersessions resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "subscribersessions": [ {

ip:<String_value>,vlan:<Integer_value>,nodeid:<Integer_value>"subscription
idtype":<String_value>,

"subscriptionidvalue":<String_value>,

"subscriberrules":<String[]_value>,
```

```
"flags":<Integer_value>,

"ttl":<Integer_value>,

"idlettl":<Integer_value>,

"avpdisplaybuffer":<String_value>,

"servicepath":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/subscribersessions? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "subscribersessions": [ { "__count": "#no"} ] }
```

system

System

System configuration.

NAME	DESCRIPTION
systemadmuserinfo	
systemautorestorefeature	Configuration for Enable/Disable the autorestore feature use to create restorepoint
systemautosaveparam	Configuration for System Autosaveparam
systembackup	Configuration for Backup Data for ns backup and restore
systemcmdpolicy	Configuration for command policy
systemcpuparam	
systemextramgmtcpu	
systemfile	Configuration for file
systemfipsstatus	Configuration for FIPS INIT Status
systemglobal_auditnslogpolicy_binding	Binding object showing the auditnslogpolicy that can be bound to systemglobal
systemglobal_auditsyslogpolicy_binding	Binding object showing the auditsyslogpolicy that can be bound to systemglobal
systemglobal_authenticationldappolicy_binding	Binding object showing the authenticationldappolicy that can be bound to systemglobal

NAME	DESCRIPTION
systemglobal_authenticationlocalpolicy_binding	Binding object showing the authenticationlocalpolicy that can be bound to systemglobal
systemglobal_authenticationpolicy_binding	Binding object showing the authenticationpolicy that can be bound to systemglobal
systemglobal_authenticationradiuspolicy_binding	Binding object showing the authenticationradiuspolicy that can be bound to systemglobal
systemglobal_authenticationtacacspolicy_binding	Binding object showing the authenticationtacacspolicy that can be bound to systemglobal
systemglobal_binding	Binding object showing the resources that can be bound to systemglobal
systemgroup	Configuration for system group
systemgroup_binding	Binding object showing the resources that can be bound to systemgroup
systemgroup_nspartition_binding	Binding object showing the nspartition that can be bound to systemgroup
systemgroup_systemcmdpolicy_binding	Binding object showing the systemcmdpolicy that can be bound to systemgroup
systemgroup_systemuser_binding	Binding object showing the systemuser that can be bound to systemgroup
systemhwerror	Configuration for Hardware errors
systemkek	Configuration for Key encryption Key
systemnsbtracing	

NAME	DESCRIPTION
systemparameter	Configuration for system parameter
systemrestorepoint	Configuration for Setting restorepoints for auto restore
systemscalablemgmtthreads	Configuration for Scalable Management Threads feature
systemsession	Configuration for system session
systemsignedexereport	Configuration for system signedExeReport
systemsshkey	
systemuser	Configuration for system user
systemuser_binding	Binding object showing the resources that can be bound to systemuser
systemuser_nspartition_binding	Binding object showing the nspartition that can be bound to systemuser
systemuser_systemcmdpolicy_binding	Binding object showing the systemcmdpolicy that can be bound to systemuser
systemuser_systemgroup_binding	Binding object showing the systemgroup that can be bound to systemuser

systemadmuserinfo

Configuration for 0 resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
username	<String>	Read-write	Name of adm-user to log in syslogs.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum length = 1

Operations

(click to see Properties)

- UPDATE

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/systemadmuserinfo **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"systemadmuserinfo":{

"username":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

systemautorestorefeature

Configuration for Enable/Disable the autorestore feature use to create restorepoint resource.

Operations

- ENABLE
- DISABLE

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ENABLE

URL: http:// <netscaler-ip-address> /nitro/v1/config/systemautorestorefeature? **action=enable**

HTTP Method: POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"systemautorestorefeature":{

}}
```

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DISABLE

URL: http:// <netscaler-ip-address> /nitro/v1/config/systemautorestorefeature? **action=disable**

HTTP Method: POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"systemautorestorefeature":{

}}
```

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

systembackup

Configuration for Backup Data for ns backup and restore resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
filename	<String>	Read-write	Name of the backup file(*.tgz) to be restored. Maximum length = 63
uselocaltimezone	<Boolean>	Read-write	This option will create backup file with local timezone timestamp.
level	<String>	Read-write	Level of data to be backed up. Default value: basic

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = basic, full
includekernel	<String>	Read-write	Use this option to add kernel in the backup file. Default value: NO Possible values = NO, YES
comment	<String>	Read-write	Comment specified at the time of creation of the backup file(*.tgz).
skipbackup	<Boolean>	Read-write	Use this option to skip taking backup during restore operation.
size	<Integer>	Read-only	Size of the backup file(*.tgz) in KB.
creationtime	<String>	Read-only	Creation time of the backup file(*.tgz).
version	<String>	Read-only	Build version of the backup file(*.tgz).
createdby	<String>	Read-only	Name of user who created the backup file(*.tgz).
ipaddress	<String>	Read-only	Ip of Citrix ADC box where the backup file(*.tgz) was created.
_nextgenapiresource	<String>	Read-only	.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- CREATE
- RESTORE
- ADD
- DELETE
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

CREATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/systembackup? **action=create HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"systembackup":{

"filename":<String_value>,

"uselocaltimezone":<Boolean_value>,

"level":<String_value>,

"includekernel":<String_value>,

"comment":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

RESTORE

URL: http:// <netscaler-ip-address> /nitro/v1/config/systembackup? **action=restore HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"systembackup":{

<b>"filename":<String_value>,

</b>"skipbackup":<Boolean_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/systembackup **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"systembackup":{

<b>"filename":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/systembackup/ filename_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/systembackup **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/systembackup? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/systembackup? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of systembackup resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/systembackup? **view=summary**

Use this query-parameter to get the summary output of systembackup resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/systembackup? **pagesize=#no;pageno=#no**

Use this query-parameter to get the systembackup resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "systembackup": [ {

"filename":<String_value>,

"level":<String_value>,

"includekernel":<String_value>,

"comment":<String_value>,

"size":<Integer_value>,

"uselocaltimezone":<Boolean_value>,

"creationtime":<String_value>,

"version":<String_value>,

"createdby":<String_value>,

"ipaddress":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/systembackup/ filename_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/systembackup/ filename_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/systembackup/ filename_value<String> ? **view=summary**

Use this query-parameter to get the summary output of systembackup resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "systembackup": [ {

"filename":<String_value>,

"level":<String_value>,

"includekernel":<String_value>,

"comment":<String_value>,

"size":<Integer_value>,

"uselocaltimezone":<Boolean_value>,

"creationtime":<String_value>,

"version":<String_value>,

"createdby":<String_value>,
```

```
"ipaddress":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/systembackup? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "systembackup": [ { "__count": "#no"} ] }
```

systemcmdpolicy

Configuration for command policy resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
policyname	<String>	Read-write	Name for a command policy.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Must begin with a letter, number, or the underscore (_) character, and must contain only alphanumeric, hyphen (-), period (.), hash (#), space ( ), at (@), equal (=), colon (:), and underscore characters. Cannot be changed after the policy is created. CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my policy" or 'my policy'). Minimum length = 1
action	<String>	Read-write	Action to perform when a request matches the policy. Possible values = ALLOW, DENY
cmdspec	<String>	Read-write	Regular expression specifying the data that matches the policy. Minimum length = 1
builtin	<String[]>	Read-only	.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL
feature	<String>	Read-only	The feature to be checked while applying this config.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of

creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/systemcmdpolicy **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"systemcmdpolicy":{

<b>"policyname":<String_value>,

</b><b>"action":<String_value>,

</b><b>"cmdspec":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/systemcmdpolicy/ policyname_value<String>
HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/systemcmdpolicy **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"systemcmdpolicy":{

<b>"policyname":<String_value>,

</b><b>"action":<String_value>,

</b><b>"cmdspec":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/systemcmdpolicy **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/systemcmdpolicy? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/systemcmdpolicy? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of systemcmdpolicy resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/systemcmdpolicy? **view=summary**

Use this query-parameter to get the summary output of systemcmdpolicy resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/systemcmdpolicy? **pagesize=#no;pageno=#no**

Use this query-parameter to get the systemcmdpolicy resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "systemcmdpolicy": [ {

"policyname":<String_value>,

"action":<String_value>,

"cmdspec":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/systemcmdpolicy/ policyname_value<String>
Query-parameters: attrs http:// <netscaler-ip-address> /nitro/v1/config/systemcmdpolicy/ policyname_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/systemcmdpolicy/ policyname_value<String> ? **view=summary**

Use this query-parameter to get the summary output of systemcmdpolicy resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "systemcmdpolicy": [ {

"policyname":<String_value>,

"action":<String_value>,

"cmdspec":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/systemcmdpolicy? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "systemcmdpolicy": [ { "__count": "#no"} ] }
```

systemcpuparam

Configuration for 0 resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
pemode	<String>	Read-write	Set PEmode to DEFAULT/ CPUBOUND. Distribute the PE weights equally if PEmode is set to CPUBOUND. Possible values = DEFAULT, CPUBOUND
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- UPDATE
- UNSET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/systemcpuparam **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"systemcpuparam":{

"pemode":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/systemcpuparam? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"systemcpuparam":{

"pemode":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/systemcpuparam **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/systemcpuparam? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/systemcpuparam? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of systemcpuparam resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/systemcpuparam? **view=summary**

Use this query-parameter to get the summary output of systemcpuparam resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/systemcpuparam? **pagesize=#no;pageno=#no**

Use this query-parameter to get the systemcpuparam resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "systemcpuparam": [ {

"pemode":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/systemcpuparam? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "systemcpuparam": [ { "__count": "#no"} ] }
```

systemextramgmtcpu

Configuration for 0 resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
nodeid	<Integer>	Read-write	Unique number that identifies the cluster node. Minimum value = 0 Maximum value = 31
configuredstate	<String>	Read-only	Get the configured state of extra management cpu. Default value: DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ENABLED, DISABLED
effectivestate	<String>	Read-only	Get the current running state of extra management cpu. Default value: DISABLED Possible values = ENABLED, DISABLED
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- ENABLE
- DISABLE
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ENABLE

URL: http:// <netscaler-ip-address> /nitro/v1/config/systemextramgmtcpu? **action=enable HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"systemextramgmtcpu":{

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DISABLE

URL: http:// <netscaler-ip-address> /nitro/v1/config/systemextramgmtcpu? **action=disable HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"systemextramgmtcpu":{

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/systemextramgmtcpu **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/systemextramgmtcpu? **args=nodeid: <Integer_value>**

Use this query-parameter to get systemextramgmtcpu resources based on additional properties.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "systemextramgmtcpu": [ {

nodeid:<Integer_value>"configuredstate":<String_value>,

"effectivestate":<String_value>,
```

```
"_nextgenapiresource":<String_value>

}]}
```

systemfile

Configuration for file resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
filename	<String>	Read-write	Name of the file. It should not include filepath. Maximum length = 255
filecontent	<String>	Read-write	file content in Base64 format.
filelocation	<String>	Read-write	location of the file on Citrix ADC. Maximum length = 255
fileencoding	<String>	Read-write	encoding type of the file content. Default value: "BASE64"
fileaccesstime	<String>	Read-only	Last access time of the file.
filemodifiedtime	<String>	Read-only	last modified time of the file.
filemode	<String[]>	Read-only	file mode.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = DIRECTORY
filesize	<Integer>	Read-only	Size of the file in BYTES.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/systemfile **Query-parameters: override** = <String_value>

HTTP Method: POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"systemfile":{

<b>"filename":<String_value>,

</b><b>"filecontent":<String_value>,

</b><b>"filelocation":<String_value>,

</b>"fileencoding":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/systemfile/ filename_value<String> **Query-parameters: args= filelocation:<String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/systemfile **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/systemfile? **args=filename: <String_value> , filelocation:<String_value>,**

Use this query-parameter to get systemfile resources based on additional properties.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "systemfile": [ {

filename:<String_value>,<b>filelocation:<String_value>,</
b>"filecontent":<String_value>,

"fileencoding":<String_value>,

"fileaccesstime":<String_value>,

"filemodifiedtime":<String_value>,
```

```
"filemode":<String[]_value>,

"filesize":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

systemfipsstatus

Configuration for FIPS INIT Status resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
fipsstatus	<String>	Read-write	Fips Initialization Status. Possible values = System is operating in FIPS mode, System is operating in non FIPS mode
netscalercontrolplanecryptographiclibraryversion	<String>	Read-write	NetScaler control plane cryptographic library version.
netscalerdataplanecryptographiclibraryversion	<String>	Read-write	NetScaler data plane cryptographic library version.
netscalercrytographicmoduleversion	<String>	Read-write	NetScaler cryptographic module version.
intelhwcryptographicacceleratorversion	<String>	Read-write	Intel hardware cryptographic accelerator version.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
netscalerjitterentropy sourceversion	<String>	Read-write	Jitter Entropy Source version.
_nextgenapiresource	<String>	Read-write	.

Operations

(click to see Properties)

- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/systemfipsstatus **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "systemfipsstatus": [ {

"fipsstatus":<String_value>,

"netscalercontrolplanecryptographiclibraryversion":<String_value>,

"netscalerdataplanecryptographiclibraryversion":<String_value>,

"netscalercrytographicmoduleversion":<String_value>,

"intelhwcryptographicacceleratorversion":<String_value>,

"netscalerjitterentropysourceversion":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

systemglobal_auditnslogpolicy_binding

Binding object showing the auditnslogpolicy that can be bound to systemglobal.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
feature	<String>	Read-write	The feature to be checked while applying this config.
gotopriorityexpression	<String>	Read-write	Applicable only to advance authentication policy. Expression or other value specifying the next policy to be evaluated if the current policy evaluates to TRUE. Specify one of the following values: * NEXT - Evaluate the policy with the next higher priority number. * END - End policy evaluation.
globalbindtype	<String>	Read-write	. Default value: SYSTEM_GLOBAL Possible values = SYSTEM_GLOBAL, VPN_GLOBAL, RNAT_GLOBAL, APPFW_GLOBAL, TM_GLOBAL
policyname	<String>	Read-write	The name of the command policy.
builtin	<String[]>	Read-write	Indicates that a variable is a built-in (SYSTEM INTERNAL) type.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL
nextfactor	<String>	Read-write	On success invoke label. Applicable for advanced authentication policy binding.
priority	<Integer>	Read-write	The priority of the command policy.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of

creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/systemglobal_auditnslogpolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"systemglobal_auditnslogpolicy_binding":{

"policyname":<String_value>,

"priority":<Integer_value>,

"nextfactor":<String_value>,

"gotopriorityexpression":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/systemglobal_auditnslogpolicy_binding **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/systemglobal_auditnslogpolicy_binding? **args=policyname: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/systemglobal_auditnslogpolicy_binding **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/systemglobal_auditnslogpolicy_binding? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of systemglobal_auditnslogpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/systemglobal_auditnslogpolicy_binding? **pagesize=#no;pageno=#no**

Use this query-parameter to get the systemglobal_auditnslogpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "systemglobal_auditnslogpolicy_binding": [ {

"feature":<String_value>,

"gotopriorityexpression":<String_value>,

"globalbindtype":<String_value>,

"policyname":<String_value>,

"builtin":<String[]_value>,

"nextfactor":<String_value>,

"priority":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/systemglobal_auditnslogpolicy_binding?**count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "systemglobal_auditnslogpolicy_binding": [ { "__count": "#no"} ] }
```

systemglobal_auditsyslogpolicy_binding

Binding object showing the auditsyslogpolicy that can be bound to systemglobal.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
priority	<Integer>	Read-write	The priority of the command policy.
builtin	<String[]>	Read-write	Indicates that a variable is a built-in (SYSTEM INTERNAL) type. Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL
nextfactor	<String>	Read-write	On success invoke label. Applicable for advanced authentication policy binding.
gotopriorityexpression	<String>	Read-write	Applicable only to advance authentication policy. Expression or other value specifying the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			next policy to be evaluated if the current policy evaluates to TRUE. Specify one of the following values: * NEXT - Evaluate the policy with the next higher priority number. * END - End policy evaluation.
policyname	<String>	Read-write	The name of the command policy.
globalbindtype	<String>	Read-write	. Default value: SYSTEM_GLOBAL Possible values = SYSTEM_GLOBAL, VPN_GLOBAL, RNAT_GLOBAL, APPFW_GLOBAL, TM_GLOBAL
feature	<String>	Read-write	The feature to be checked while applying this config.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/systemglobal_auditsyslogpolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"systemglobal_auditsyslogpolicy_binding":{
```

```
"policyname":<String_value>,

"priority":<Integer_value>,

"nextfactor":<String_value>,

"gotopriorityexpression":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/systemglobal_auditsyslogpolicy_binding **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/systemglobal_auditsyslogpolicy_binding? **args=policyname: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/systemglobal_auditsyslogpolicy_binding **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/systemglobal_auditsyslogpolicy_binding? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of systemglobal_auditsyslogpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/systemglobal_auditsyslogpolicy_binding? **pagesize=#no;pageno=#no**

Use this query-parameter to get the systemglobal_auditsyslogpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "systemglobal_auditsyslogpolicy_binding": [ {

"priority":<Integer_value>,

"builtin":<String[]_value>,

"nextfactor":<String_value>,

"gotopriorityexpression":<String_value>,

"policyname":<String_value>,

"globalbindtype":<String_value>,

"feature":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/systemglobal_auditsyslogpolicy_binding?**count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "systemglobal_auditsyslogpolicy_binding": [ { "__count": "#no"} ] }
```

systemglobal_authenticationldappolicy_binding

Binding object showing the authenticationldappolicy that can be bound to systemglobal.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
builtin	<String[]>	Read-write	Indicates that a variable is a built-in (SYSTEM INTERNAL) type. Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
nextfactor	<String>	Read-write	On success invoke label. Applicable for advanced authentication policy binding.
gotopriorityexpression	<String>	Read-write	Applicable only to advance authentication policy. Expression or other value specifying the next policy to be evaluated if the current policy evaluates to TRUE. Specify one of the following values: * NEXT - Evaluate the policy with the next higher priority number. * END - End policy evaluation.
policyname	<String>	Read-write	The name of the command policy.
globalbindtype	<String>	Read-write	. Default value: SYSTEM_GLOBAL Possible values = SYSTEM_GLOBAL, VPN_GLOBAL, RNAT_GLOBAL, APPFW_GLOBAL, TM_GLOBAL
feature	<String>	Read-write	The feature to be checked while applying this config.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
priority	<Integer>	Read-write	The priority of the command policy.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/systemglobal_authenticationldappolicy_binding
HTTP Method: PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"systemglobal_authenticationldappolicy_binding":{

"policyname":<String_value>,

"priority":<Integer_value>,

"nextfactor":<String_value>,

"gotopriorityexpression":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/systemglobal_authenticationldappolicy_binding
Query-parameters: args http:// <netscaler-ip-address> /nitro/v1/config/systemglobal_authenticationldappolicy_binding? **args=policyname: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/systemglobal_authenticationldappolicy_binding **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/systemglobal_authenticationldappolicy_binding? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of systemglobal_authenticationldappolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/systemglobal_authenticationldappolicy_binding? **pagesize=#no;pageno=#no**

Use this query-parameter to get the systemglobal_authenticationldappolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "systemglobal_authenticationldappolicy_binding": [ {

"builtin":<String[]_value>,
```

```
"nextfactor":<String_value>,

"gotopriorityexpression":<String_value>,

"policyname":<String_value>,

"globalbindtype":<String_value>,

"feature":<String_value>,

"priority":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/ systemglobal_authenticationldappolicy_binding? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "systemglobal_authenticationldappolicy_binding": [ { "__count":
"#no"} ] }
```

systemglobal_authenticationlocalpolicy_binding

Binding object showing the authenticationlocalpolicy that can be bound to systemglobal.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
priority	<Integer>	Read-write	The priority of the command policy.
builtin	<String[]>	Read-write	Indicates that a variable is a built-in (SYSTEM INTERNAL) type. Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL
nextfactor	<String>	Read-write	On success invoke label. Applicable for advanced authentication policy binding.
feature	<String>	Read-write	The feature to be checked while applying this config.
gotopriorityexpression	<String>	Read-write	Applicable only to advance authentication policy. Expression or other value specifying the next policy to be evaluated if the current policy evaluates to TRUE. Specify one of the following values: *

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			NEXT - Evaluate the policy with the next higher priority number. * END - End policy evaluation.
policyname	<String>	Read-write	The name of the command policy.
globalbindtype	<String>	Read-write	. Default value: SYSTEM_GLOBAL Possible values = SYSTEM_GLOBAL, VPN_GLOBAL, RNAT_GLOBAL, APPFW_GLOBAL, TM_GLOBAL
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/systemglobal_authenticationlocalpolicy_binding
HTTP Method: PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"systemglobal_authenticationlocalpolicy_binding":{

"policyname":<String_value>,

"priority":<Integer_value>,

"nextfactor":<String_value>,

"gotopriorityexpression":<String_value>
```

```
}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/systemglobal_authenticationlocalpolicy_binding **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/systemglobal_authenticationlocalpolicy_binding? **args=policyname: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/systemglobal_authenticationlocalpolicy_binding **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/systemglobal_authenticationlocalpolicy_binding? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of systemglobal_authenticationlocalpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/systemglobal_authenticationlocalpolicy_binding? **pagesize=#no;pageno=#no**

Use this query-parameter to get the systemglobal_authenticationlocalpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "systemglobal_authenticationlocalpolicy_binding": [ {

"priority":<Integer_value>,

"builtin":<String[]_value>,

"nextfactor":<String_value>,

"feature":<String_value>,

"gotopriorityexpression":<String_value>,

"policyname":<String_value>,

"globalbindtype":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/ systemglobal_authenticationlocalpolicy_binding? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "systemglobal_authenticationlocalpolicy_binding": [ { "__count":
"#no"} ] }
```

systemglobal_authenticationpolicy_binding

Binding object showing the authenticationpolicy that can be bound to systemglobal.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
nextfactor	<String>	Read-write	On success invoke label. Applicable for advanced authentication policy binding.
builtin	<String[]>	Read-write	Indicates that a variable is a built-in (SYSTEM INTERNAL) type. Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
feature	<String>	Read-write	The feature to be checked while applying this config.
policyname	<String>	Read-write	The name of the command policy.
globalbindtype	<String>	Read-write	. Default value: SYSTEM_GLOBAL Possible values = SYSTEM_GLOBAL, VPN_GLOBAL, RNAT_GLOBAL, APPFW_GLOBAL, TM_GLOBAL
gotopriorityexpression	<String>	Read-write	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE. Applicable only for advanced authentication policies.
priority	<Integer>	Read-write	The priority of the command policy.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD

- DELETE
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/systemglobal_authenticationpolicy_binding
HTTP Method: PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"systemglobal_authenticationpolicy_binding":{

"policyname":<String_value>,

"priority":<Integer_value>,

"nextfactor":<String_value>,

"gotopriorityexpression":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/systemglobal_authenticationpolicy_binding **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/systemglobal_authenticationpolicy_binding? **args=policyname: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/systemglobal_authenticationpolicy_binding **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/systemglobal_authenticationpolicy_binding? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of systemglobal_authenticationpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ systemglobal_authenticationpolicy_binding? **pagesize=#no;pageno=#no**

Use this query-parameter to get the systemglobal_authenticationpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "systemglobal_authenticationpolicy_binding": [ {

"nextfactor":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"policyname":<String_value>,

"globalbindtype":<String_value>,

"gotopriorityexpression":<String_value>,

"priority":<Integer_value>
```

```
}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/systemglobal_authenticationpolicy_binding?**count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "systemglobal_authenticationpolicy_binding": [ { "__count": "#no"} ] }
```

systemglobal_authenticationradiuspolicy_binding

Binding object showing the authenticationradiuspolicy that can be bound to systemglobal.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
priority	<Integer>	Read-write	The priority of the command policy.
feature	<String>	Read-write	The feature to be checked while applying this config.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
gotopriorityexpression	<String>	Read-write	Applicable only to advance authentication policy. Expression or other value specifying the next policy to be evaluated if the current policy evaluates to TRUE. Specify one of the following values: * NEXT - Evaluate the policy with the next higher priority number. * END - End policy evaluation.
policyname	<String>	Read-write	The name of the command policy.
globalbindtype	<String>	Read-write	. Default value: SYSTEM_GLOBAL Possible values = SYSTEM_GLOBAL, VPN_GLOBAL, RNAT_GLOBAL, APPFW_GLOBAL, TM_GLOBAL
builtin	<String[]>	Read-write	Indicates that a variable is a built-in (SYSTEM INTERNAL) type. Possible values = MODIFIABLE, DELETABLE,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			IMMUTABLE, PARTITION_ALL
nextfactor	<String>	Read-write	On success invoke label. Applicable for advanced authentication policy binding.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/systemglobal_authenticationradiuspolicy_binding
HTTP Method: PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"systemglobal_authenticationradiuspolicy_binding":{

"policyname":<String_value>,

"priority":<Integer_value>,

"nextfactor":<String_value>,

"gotopriorityexpression":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/ systemglobal_authenticationradiuspolicy_binding **Query-parameters: args** http:// <netscaler-ip-

address> /nitro/v1/config/systemglobal_authenticationradiuspolicy_binding? **args=policyname: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/systemglobal_authenticationradiuspolicy_binding **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/systemglobal_authenticationradiuspolicy_binding? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of systemglobal_authenticationradiuspolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/systemglobal_authenticationradiuspolicy_binding? **pagesize=#no;pageno=#no**

Use this query-parameter to get the systemglobal_authenticationradiuspolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "systemglobal_authenticationradiuspolicy_binding": [ {

"priority":<Integer_value>,

"feature":<String_value>,

"gotopriorityexpression":<String_value>,

"policyname":<String_value>,

"globalbindtype":<String_value>,

"builtin":<String[]_value>,

"nextfactor":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/ systemglobal_authenticationradiuspolicy_binding? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "systemglobal_authenticationradiuspolicy_binding": [ { "__count":
"#no"} ] }
```

systemglobal_authenticationtacacspolicy_binding

Binding object showing the authenticationtacacspolicy that can be bound to systemglobal.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
globalbindtype	<String>	Read-write	. Default value: SYSTEM_GLOBAL Possible values = SYSTEM_GLOBAL, VPN_GLOBAL, RNAT_GLOBAL, APPFW_GLOBAL, TM_GLOBAL
policyname	<String>	Read-write	The name of the command policy.
gotopriorityexpression	<String>	Read-write	Applicable only to advance authentication policy. Expression or other value specifying the next policy to be evaluated if the current policy evaluates to TRUE. Specify one of the following values: * NEXT - Evaluate the policy with the next higher priority

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			number. * END - End policy evaluation.
feature	<String>	Read-write	The feature to be checked while applying this config.
nextfactor	<String>	Read-write	On success invoke label. Applicable for advanced authentication policy binding.
builtin	<String[]>	Read-write	Indicates that a variable is a built-in (SYSTEM INTERNAL) type. Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL
priority	<Integer>	Read-write	The priority of the command policy.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/ systemglobal_authenticationtacacspolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"systemglobal_authenticationtacacspolicy_binding":{

"policyname":<String_value>,
```

```
"priority":<Integer_value>,

"nextfactor":<String_value>,

"gotopriorityexpression":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/systemglobal_authenticationtacacspolicy_binding **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/systemglobal_authenticationtacacspolicy_binding? **args=policyname: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/systemglobal_authenticationtacacspolicy_binding **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/systemglobal_authenticationtacacspolicy_binding? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of systemglobal_authenticationtacacspolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ systemglobal_authenticationtacacspolicy_binding? **pagesize=#no;pageno=#no**

Use this query-parameter to get the systemglobal_authenticationtacacspolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "systemglobal_authenticationtacacspolicy_binding": [ {

"globalbindtype":<String_value>,

"policyname":<String_value>,

"gotopriorityexpression":<String_value>,

"feature":<String_value>,

"nextfactor":<String_value>,

"builtin":<String[]_value>,

"priority":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/ systemglobal_authenticationtacacspolicy_binding? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "systemglobal_authenticationtacacspolicy_binding": [ { "__count":
"#no"} ] }
```

systemglobal_binding

Binding object which returns the resources bound to systemglobal.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
systemglobal_auditsyslogpolicy_binding	<systemglobal_auditsyslogpolicy_binding[]>	Read-write	auditsyslogpolicy that can be bound to systemglobal.
systemglobal_authenticationlocalpolicy_binding	<systemglobal_authenticationlocalpolicy_binding[]>	Read-write	authenticationlocalpolicy that can be bound to systemglobal.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
systemglobal_authenticationldappolicy_binding	<systemglobal_authenticationldappolicy_binding[]>	Read-write	authenticationldappolicy that can be bound to systemglobal.
systemglobal_authenticationradiuspolicy_binding	<systemglobal_authenticationradiuspolicy_binding[]>	Read-write	authenticationradiuspolicy that can be bound to systemglobal.
systemglobal_authenticationtacacspolicy_binding	<systemglobal_authenticationtacacspolicy_binding[]>	Read-write	authenticationtacacspolicy that can be bound to systemglobal.
systemglobal_auditnslogpolicy_binding	<systemglobal_auditnslogpolicy_binding[]>	Read-write	auditnslogpolicy that can be bound to systemglobal.
systemglobal_authenticationpolicy_binding	<systemglobal_authenticationpolicy_binding[]>	Read-write	authenticationpolicy that can be bound to systemglobal.

Operations

(click to see Properties)

- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of

creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/systemglobal_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "systemglobal_binding": [ {

"systemglobal_auditsyslogpolicy_binding":<systemglobal_auditsyslogpolicy_b
inding[]_value>,

"systemglobal_authenticationldappolicy_binding":<systemglobal_authenticati
onldappolicy_binding[]_value>,

"systemglobal_auditnslogpolicy_binding":<systemglobal_auditnslogpolicy_bin
```

```
ding[]_value>,

"systemglobal_authenticationtacacspolicy_binding":<systemglobal_authentica
tiontacacspolicy_binding[]_value>,

"systemglobal_authenticationlocalpolicy_binding":<systemglobal_authenticat
ionlocalpolicy_binding[]_value>,

"systemglobal_authenticationpolicy_binding":<systemglobal_authenticationpo
licy_binding[]_value>,

"systemglobal_authenticationradiuspolicy_binding":<systemglobal_authentica
tionradiuspolicy_binding[]_value>

}]}
```

systemgroup

Configuration for system group resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
groupname	<String>	Read-write	Name for the group. Must begin with a letter, number, hash(#) or the underscore (_) character, and must contain only alphanumeric, hyphen (-), period (.), hash (#), space ( ), at (@), equal (=), colon (:), and underscore characters. Cannot be changed after the group is created.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my group" or 'my group'). Minimum length = 1
promptstring	<String>	Read-write	String to display at the command-line prompt. Can consist of letters, numbers, hyphen (-), period (.), hash (#), space ( ), at (@), equal (=), colon (:), underscore (_), and the following variables: * %u - Will be replaced by the user name. * %h - Will be replaced by the hostname of the Citrix ADC. * %t - Will be replaced by the current time in 12-hour format. * %T - Will be replaced by the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			current time in 24-hour format. * %d - Will be replaced by the current date. * %s - Will be replaced by the state of the Citrix ADC. Note: The 63-character limit for the length of the string does not apply to the characters that replace the variables. Minimum length = 1
timeout	<Integer>	Read-write	CLI session inactivity timeout, in seconds. If Restrictedtimeout argument of system parameter is enabled, Timeout can have values in the range [300-86400] seconds.If Restrictedtimeout argument of system parameter is disabled, Timeout can have values in the range [0, 10-100000000]

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			seconds. Default value is 900 seconds.
allowedmanagementinterface	<String[]>	Read-write	Allowed Management interfaces of the system users in the group. By default allowed from both API and CLI interfaces. If management interface for a group is set to API, then all users under this group will not allowed to access NS through CLI. GUI interface will come under API interface. Default value: NS_INTERFACE_ALL Possible values = CLI, API
daystoexpire	<Integer>	Read-write	Password days to expire for system groups. The daystoexpire value ranges from 30 to 255. Minimum value = 30 Maximum value = 255

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
warnpriorndays	<Integer>	Read-write	Number of days before which password expiration warning would be thrown with respect to daystoexpire. The warnpriorndays value ranges from 5 to 40. Minimum value = 5 Maximum value = 40
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET (ALL)
- GET
- COUNT
- UPDATE
- UNSET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/systemgroup **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"systemgroup":{

<b>"groupname":<String_value>,

</b>"promptstring":<String_value>,

"timeout":<Integer_value>,

"allowedmanagementinterface":<String[]_value>,

"daystoexpire":<Integer_value>,

"warnpriorndays":<Integer_value>
```

```
}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/systemgroup/ groupname_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/systemgroup **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"systemgroup":{

<b>"groupname":<String_value>,

</b>"promptstring":<String_value>,

"timeout":<Integer_value>,

"allowedmanagementinterface":<String[]_value>,

"daystoexpire":<Integer_value>,
```

```
"warnpriorndays":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/systemgroup? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"systemgroup":{

<b>"groupname":<String_value>,

</b>"promptstring":true,

"timeout":true,

"allowedmanagementinterface":true,

"daystoexpire":true,

"warnpriorndays":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/systemgroup **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/systemgroup? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/systemgroup? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of systemgroup resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/systemgroup? **view=summary**

Use this query-parameter to get the summary output of systemgroup resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/systemgroup? **pagesize=#no;pageno=#no**

Use this query-parameter to get the systemgroup resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "systemgroup": [ {

"groupname":<String_value>,

"promptstring":<String_value>,

"timeout":<Integer_value>,

"allowedmanagementinterface":<String[]_value>,

"daystoexpire":<Integer_value>,

"warnpriorndays":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/systemgroup/ groupname_value<String>
Query-parameters: attrs http:// <netscaler-ip-address> /nitro/v1/config/systemgroup/ groupname_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/systemgroup/ groupname_value<String> ? **view=summary**

Use this query-parameter to get the summary output of systemgroup resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "systemgroup": [ {

"groupname":<String_value>,

"promptstring":<String_value>,

"timeout":<Integer_value>,

"allowedmanagementinterface":<String[]_value>,

"daystoexpire":<Integer_value>,

"warnpriorndays":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/systemgroup? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "systemgroup": [ { "__count": "#no"} ] }
```

systemgroup_binding

Binding object which returns the resources bound to systemgroup.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
groupname	<String>	Read-write	Name of the system group about which to display information. Minimum length = 1
systemgroup_systemcmdpolicy_binding	<systemgroup_systemcmdpolicy_binding[]>	Read-only	systemcmdpolicy that can be bound to systemgroup.
systemgroup_systemuser_binding	<systemgroup_systemuser_binding[]>	Read-only	systemuser that can be bound to systemgroup.
systemgroup_nspartition_binding	<systemgroup_nspartition_binding[]>	Read-only	nspartition that can be bound to systemgroup.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/systemgroup_binding/groupname_value<String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "systemgroup_binding": [ {

"groupname":<String_value>,

"systemgroup_nspartition_binding":<systemgroup_nspartition_binding[]_value
>,

"systemgroup_systemuser_binding":<systemgroup_systemuser_binding[]_value>,

"systemgroup_systemcmdpolicy_binding":<systemgroup_systemcmdpolicy_binding
[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/systemgroup_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/systemgroup_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "systemgroup_binding": [ {

"groupname":<String_value>,

"systemgroup_nspartition_binding":<systemgroup_nspartition_binding[]_value
>,

"systemgroup_systemuser_binding":<systemgroup_systemuser_binding[]_value>,

"systemgroup_systemcmdpolicy_binding":<systemgroup_systemcmdpolicy_binding
[]_value>

}]}
```

systemgroup_nspartition_binding

Binding object showing the nspartition that can be bound to systemgroup.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
partitionname	<String>	Read-write	Name of the Partition to bind to the system group. Minimum length = 1
groupname	<String>	Read-write	Name of the system group. Minimum length = 1
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET

- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/systemgroup_nspartition_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"systemgroup_nspartition_binding":{

<b>"groupname":<String_value>,

</b>"partitionname":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/systemgroup_nspartition_binding/ groupname_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ systemgroup_nspartition_binding/ groupname_value<String> ? **args=partitionname: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/systemgroup_nspartition_binding/ groupname_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ systemgroup_nspartition_binding/ groupname_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of systemgroup_nspartition_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/systemgroup_nspartition_binding/groupname_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the systemgroup_nspartition_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "systemgroup_nspartition_binding": [ {

"partitionname":<String_value>,

"groupname":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/systemgroup_nspartition_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/systemgroup_nspartition_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "systemgroup_nspartition_binding": [ {

"partitionname":<String_value>,

"groupname":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/systemgroup_nspartition_binding/groupname_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"systemgroup_nspartition_binding": [ { "__count": "#no"} ] }
```

systemgroup_systemcmdpolicy_binding

Binding object showing the systemcmdpolicy that can be bound to systemgroup.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
priority	<Integer>	Read-write	The priority of the command policy.
groupname	<String>	Read-write	Name of the system group. Minimum length = 1
policyname	<String>	Read-write	The name of command policy.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/systemgroup_systemcmdpolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"systemgroup_systemcmdpolicy_binding":{

<b>"groupname":<String_value>,
```

```
</b>"policyname":<String_value>,

"priority":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/systemgroup_systemcmdpolicy_binding/ groupname_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ systemgroup_systemcmdpolicy_binding/ groupname_value<String> ? **args=policyname: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/systemgroup_systemcmdpolicy_binding/ groupname_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ systemgroup_systemcmdpolicy_binding/ groupname_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of systemgroup_systemcmdpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/systemgroup_systemcmdpolicy_binding/ groupname_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the systemgroup_systemcmdpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "systemgroup_systemcmdpolicy_binding": [ {

"priority":<Integer_value>,

"groupname":<String_value>,

"policyname":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/systemgroup_systemcmdpolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/systemgroup_systemcmdpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "systemgroup_systemcmdpolicy_binding": [ {

"priority":<Integer_value>,

"groupname":<String_value>,

"policyname":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/systemgroup_systemcmdpolicy_binding/ groupname_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"systemgroup_systemcmdpolicy_binding": [ { "__count": "#no"} ] }
```

systemgroup_systemuser_binding

Binding object showing the systemuser that can be bound to systemgroup.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
username	<String>	Read-write	The system user.
groupname	<String>	Read-write	Name of the system group. Minimum length = 1
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/systemgroup_systemuser_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"systemgroup_systemuser_binding":{

<b>"groupname":<String_value>,

</b>"username":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/systemgroup_systemuser_binding/ groupname_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ systemgroup_systemuser_binding/ groupname_value<String> ? **args=username: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/systemgroup_systemuser_binding/ groupname_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ systemgroup_systemuser_binding/ groupname_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of systemgroup_systemuser_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/systemgroup_systemuser_binding/ groupname_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the systemgroup_systemuser_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "systemgroup_systemuser_binding": [ {

"username":<String_value>,

"groupname":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/systemgroup_systemuser_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/systemgroup_systemuser_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "systemgroup_systemuser_binding": [ {

"username":<String_value>,

"groupname":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/systemgroup_systemuser_binding/ groupname_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"systemgroup_systemuser_binding": [ { "__count": "#no"} ] }
```

systemhwerror

Configuration for Hardware errors resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
diskcheck	<Boolean>	Read-write	Perform only disk error checking.
response	<String>	Read-only	Response captured during hardware examination.
hwerrorcount	<Integer>	Read-only	Number of errors found. Check response field for more information on errors if this value is non zero.

Operations

(click to see Properties)

- CHECK

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

CHECK

URL: http:// <netscaler-ip-address> /nitro/v1/config/systemhwerror? **action=check**

HTTP Method: POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"systemhwerror":{

<b>"diskcheck":<Boolean_value>

</b>}}
```

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Payload:

```
{ "systemhwerror": [ {

"response":<String_value>,

"hwerrorcount":<Integer_value>
```

```
}]}
```

systemkek

Configuration for Key encryption Key resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
level	<String>	Read-write	Type of update KEK to be performed. *basic : The level basic will backup old keys and create new keys and respond back. *extended : The level extended will backup old keys and create new keys, update ns.conf, nscfg.db, all ns.conf for same release, in all partitions. While doing so will block all config changes and once done shall respond back.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = basic, extended

Operations

(click to see Properties)

- CHANGE

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

CHANGE

URL: http:// <netscaler-ip-address> /nitro/v1/config/systemkek? **action=update HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"systemkek":{

<b>"level":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

systemnsbtracing

Configuration for 0 resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
nodeid	<Integer>	Read-write	Unique number that identifies the cluster node. Minimum value = 0 Maximum value = 31
configuredstate	<String>	Read-only	Get the configured state of nsb tracing. Default value: DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ENABLED, DISABLED
effectivestate	<String>	Read-only	Get the current running state of nsb tracing. Default value: DISABLED Possible values = ENABLED, DISABLED
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- ENABLE
- DISABLE
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ENABLE

URL: http:// <netscaler-ip-address> /nitro/v1/config/systemnsbtracing? **action=enable HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"systemnsbtracing":{

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DISABLE

URL: http:// <netscaler-ip-address> /nitro/v1/config/systemnsbtracing? **action=disable HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"systemnsbtracing":{

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/systemnsbtracing **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/systemnsbtracing? **args=nodeid: <Integer_value>**

Use this query-parameter to get systemnsbtracing resources based on additional properties.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "systemnsbtracing": [ {

nodeid:<Integer_value>"configuredstate":<String_value>,

"effectivestate":<String_value>,

"_nextgenapiresource":<String_value>
```

```
}]}
```

systemparameter

Configuration for system parameter resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
rbaonresponse	<String>	Read-write	Enable or disable Role-Based Authentication (RBA) on responses. Default value: ENABLED Possible values = ENABLED, DISABLED
promptstring	<String>	Read-write	String to display at the command-line prompt. Can consist of letters, numbers, hyphen (-), period (.), hash (#), space ( ), at (@), equal (=), colon (:), underscore (_), and the following variables: * %u - Will be replaced by the user name. * %h - Will be replaced by the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			hostname of the Citrix ADC. * %t - Will be replaced by the current time in 12-hour format. * %T - Will be replaced by the current time in 24-hour format. * %d - Will be replaced by the current date. * %s - Will be replaced by the state of the Citrix ADC. Note: The 63-character limit for the length of the string does not apply to the characters that replace the variables. Minimum length = 1
natpcbforceflushlimit	<Integer>	Read-write	Flush the system if the number of Network Address Translation Protocol Control Blocks

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			(NATPCBs) exceeds this value. Default value: 2147483647 Minimum value = 1000
natpcbrstontimeout	<String>	Read-write	Send a reset signal to client and server connections when their NATPCBs time out. Avoids the buildup of idle TCP connections on both the sides. Default value: DISABLED Possible values = ENABLED, DISABLED
timeout	<Integer>	Read-write	CLI session inactivity timeout, in seconds. If Restrictedtimeout argument is enabled, Timeout can have values in the range [300-86400] seconds. If Restrictedtimeout argument is disabled, Timeout can have values in the range [0, 10-100000000] seconds. Default

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			value is 900 seconds.
localauth	<String>	Read-write	When enabled, local users can access Citrix ADC even when external authentication is configured. When disabled, local users are not allowed to access the Citrix ADC, Local users can access the Citrix ADC only when the configured external authentication servers are unavailable. This parameter is not applicable to SSH Key-based authentication. Default value: ENABLED Possible values = ENABLED, DISABLED
minpasswordlen	<Integer>	Read-write	Minimum length of system user password. When strong password is enabled default minimum length is 8. User entered value can be greater than or equal to 8. Default mininum value is 1 when strong

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			password is disabled. Maximum value is 127 in both cases. Minimum value = 1 Maximum value = 127
strongpassword	<String>	Read-write	After enabling strong password (enableall / enablelocal - not included in exclude list), all the passwords / sensitive information must have - Atleast 1 Lower case character, Atleast 1 Upper case character, Atleast 1 numeric character, Atleast 1 special character (~, `, !, @, #, $, %, \^, ;, *, -, _, =, +, {, }, [,], |, \, :, <, >, /, ., ,, " "). Exclude list in case of enablelocal is - NS_FIPS, NS_CRL, NS_RSAKEY, NS_PKCS12, NS_PKCS8, NS_LDAP, NS_TACACS, NS_TACACSACTION, NS_RADIUS, NS_RADIUSACTION, NS_ENCRYPTION_PARAMS. So no

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Strong Password checks will be performed on these ObjectType commands for enablelocal case. Default value: disabled Possible values = enableall, enablelocal, disabled
restrictedtimeout	<String>	Read-write	Enable/Disable the restricted timeout behaviour. When enabled, timeout cannot be configured beyond admin configured timeout and also it will have the [minimum - maximum] range check. When disabled, timeout will have the old behaviour. By default the value is disabled. Default value: DISABLED Possible values = ENABLED, DISABLED
fipsusermode	<String>	Read-write	Use this option to set the FIPS mode for key user-land processes. When

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			enabled, these user-land processes will operate in FIPS mode. In this mode, these processes will use FIPS 140-2 certified crypto algorithms. With a FIPS license, it is enabled by default and cannot be disabled. Without a FIPS license, it is disabled by default, wherein these user-land processes will not operate in FIPS mode. Default value: DISABLED Possible values = ENABLED, DISABLED
doppler	<String>	Read-write	Enable or disable Doppler. Default value: ENABLED Possible values = ENABLED, DISABLED
googleanalytics	<String>	Read-write	Enable or disable Google analytics.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: DISABLED Possible values = ENABLED, DISABLED
totalauthtimeout	<Integer>	Read-write	Total time a request can take for authentication/ authorization. Default value: 20 Minimum value = 5 Maximum value = 120
cliloglevel	<String>	Read-write	Audit log level, which specifies the types of events to log for cli executed commands. Available values function as follows: * EMERGENCY - Events that indicate an immediate crisis on the server. * ALERT - Events that might require action. * CRITICAL - Events that indicate an imminent server crisis.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			* ERROR - Events that indicate some type of error. * WARNING - Events that require action in the near future. * NOTICE - Events that the administrator should know about. * INFORMATIONAL - All but low-level events. * DEBUG - All events, in extreme detail. Default value: INFORMATIONAL Possible values = EMERGENCY, ALERT, CRITICAL, ERROR, WARNING, NOTICE, INFORMATIONAL, DEBUG
forcepasswordchange	<String>	Read-write	Enable or disable force password change for nsroot user.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: DISABLED Possible values = ENABLED, DISABLED
basicauth	<String>	Read-write	Enable or disable basic authentication for Nitro API. Default value: ENABLED Possible values = ENABLED, DISABLED
reauthonauthparamchange	<String>	Read-write	Enable or disable External user reauthentication when authentication parameter changes. Default value: DISABLED Possible values = ENABLED, DISABLED
removesensitivefiles	<String>	Read-write	Use this option to remove the sensitive files from the system like authorise keys, public keys etc. The commands which will remove sensitive files when this system paramter is enabled are rm cluster instance, rm

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			cluster node, rm ha node, clear config full, join cluster and add cluster instance. Default value: DISABLED Possible values = ENABLED, DISABLED
maxsessionperuser	<Integer>	Read-write	Maximum number of client connection allowed per user.The maxsessionperuser value ranges from 1 to 40. Minimum value = 1 Maximum value = 40
wafprotection	<String[]>	Read-write	Configure WAF protection for endpoints used by NetScaler management interfaces. The available options are: * DEFAULT - NetScaler decides which endpoints have WAF protection enabled. * GUI - Endpoints used by the Management GUI

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Interface are WAF protected. * DISABLED - WAF protection is disabled. Default value: DEFAULT Possible values = DEFAULT, DISABLED, GUI
denylist	<String>	Read-write	Enable or disable denylist protection. The available options are: * ON - Denylist feature is enabled. * OFF - Denylist feature is disabled. Default value: ON Possible values = ON, OFF
denylistlogging	<String>	Read-write	Enable or disable denylist protection logging. The available options are: * ON - Denylist logging is enabled. * OFF - Denylist logging is disabled. Default value: OFF

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ON, OFF
passwordhistorycontrol	<String>	Read-write	Enables or disable password expiry feature for system users. If the feature is ENABLED, by default the last 6 passwords of users will be maintained and will not be allowed to reuse same. When the feature is enabled the daystoexpire, warnpriorndays and pwdhistoryCount will be set with default values. The values can only be set in system for system parameter. It cannot be unset. It is possible to set and unset the values for daytoexpire and warnpriorndays in system groups.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default values if feature is ENABLED: daystoexpire: 30 warnpriorndays: 5 pwdhistoryCount: 6 If the feature is DISABLED the values cannot be set or unset in system parameter and system groups. Default value: DISABLED Possible values = ENABLED, DISABLED
daystoexpire	<Integer>	Read-write	Password expiry days for all the system users. The daystoexpire value ranges from 30 to 255. Minimum value = 30 Maximum value = 255
warnpriorndays	<Integer>	Read-write	Number of days before which password expiration warning would be thrown with respect to daystoexpire. The

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			warnpriorndays value ranges from 5 to 40. Minimum value = 5 Maximum value = 40
pwdhistorycount	<Integer>	Read-write	Number of passwords to be maintained as history for system users. The pwdhistorycount value ranges from 1 to 10. Minimum value = 1 Maximum value = 10
maxclient	<Integer>	Read-only	Maximum number of client connection allowed by the system. Minimum value = 10 Maximum value = 40
allowdefaultpartition	<String>	Read-only	Enable/Disable the allowing partition users to access default partition. Default value: NO Possible values = YES, NO
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- UPDATE
- UNSET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/systemparameter **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"systemparameter":{

"rbaonresponse":<String_value>,

"promptstring":<String_value>,

"natpcbforceflushlimit":<Integer_value>,

"natpcbrstontimeout":<String_value>,

"timeout":<Integer_value>,

"localauth":<String_value>,

"minpasswordlen":<Integer_value>,

"strongpassword":<String_value>,

"restrictedtimeout":<String_value>,

"fipsusermode":<String_value>,

"doppler":<String_value>,

"googleanalytics":<String_value>,

"totalauthtimeout":<Integer_value>,

"cliloglevel":<String_value>,

"forcepasswordchange":<String_value>,

"basicauth":<String_value>,

"reauthonauthparamchange":<String_value>,

"removesensitivefiles":<String_value>,

"maxsessionperuser":<Integer_value>,

"wafprotection":<String[]_value>,
```

```
"denylist":<String_value>,

"denylistlogging":<String_value>,

"passwordhistorycontrol":<String_value>,

"daystoexpire":<Integer_value>,

"warnpriorndays":<Integer_value>,

"pwdhistorycount":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/systemparameter? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"systemparameter":{

"minpasswordlen":true,

"rbaonresponse":true,

"promptstring":true,

"natpcbforceflushlimit":true,
```

```
"natpcbrstontimeout":true,

"timeout":true,

"localauth":true,

"strongpassword":true,

"restrictedtimeout":true,

"fipsusermode":true,

"doppler":true,

"googleanalytics":true,

"totalauthtimeout":true,

"cliloglevel":true,

"forcepasswordchange":true,

"basicauth":true,

"reauthonauthparamchange":true,

"removesensitivefiles":true,

"maxsessionperuser":true,

"wafprotection":true,

"denylist":true,

"denylistlogging":true,

"passwordhistorycontrol":true,

"daystoexpire":true,

"warnpriorndays":true,

"pwdhistorycount":true
```

```
}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/systemparameter **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "systemparameter": [ {

"rbaonresponse":<String_value>,

"promptstring":<String_value>,

"natpcbforceflushlimit":<Integer_value>,

"natpcbrstontimeout":<String_value>,

"timeout":<Integer_value>,

"maxclient":<Integer_value>,

"localauth":<String_value>,
```

```
"minpasswordlen":<Integer_value>,

"strongpassword":<String_value>,

"restrictedtimeout":<String_value>,

"fipsusermode":<String_value>,

"doppler":<String_value>,

"googleanalytics":<String_value>,

"cliloglevel":<String_value>,

"forcepasswordchange":<String_value>,

"totalauthtimeout":<Integer_value>,

"basicauth":<String_value>,

"allowdefaultpartition":<String_value>,

"reauthonauthparamchange":<String_value>,

"removesensitivefiles":<String_value>,

"maxsessionperuser":<Integer_value>,

"wafprotection":<String[]_value>,

"denylist":<String_value>,

"denylistlogging":<String_value>,

"passwordhistorycontrol":<String_value>,

"daystoexpire":<Integer_value>,

"warnpriorndays":<Integer_value>,

"pwdhistorycount":<Integer_value>,

"_nextgenapiresource":<String_value>
```

```
}]}
```

systemrestorepoint

Configuration for Setting restorepoints for auto restore resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
filename	<String>	Read-write	Name of the restore point. Minimum length = 1 Maximum length = 63
backupfilename	<String>	Read-only	backup file name of the restore points created internally.
techsuprtname	<String>	Read-only	Tech support bundle name created during creation of restore points.
creationtime	<String>	Read-only	Creation time of the restore points.
version	<String>	Read-only	Build version of the restore points.
createdby	<String>	Read-only	Name of user who created the restore points.
ipaddress	<String>	Read-only	Ip of Netscaler box where the restore point was created.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- CREATE
- DELETE
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

CREATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/systemrestorepoint? **action=create HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"systemrestorepoint":{

<b>"filename":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/systemrestorepoint/ filename_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/systemrestorepoint **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/systemrestorepoint? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/systemrestorepoint? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of systemrestorepoint resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/systemrestorepoint? **view=summary**

Use this query-parameter to get the summary output of systemrestorepoint resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/systemrestorepoint? **pagesize=#no;pageno=#no**

Use this query-parameter to get the systemrestorepoint resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "systemrestorepoint": [ {

"filename":<String_value>,

"backupfilename":<String_value>,
```

```
"techsuprtname":<String_value>,

"creationtime":<String_value>,

"version":<String_value>,

"createdby":<String_value>,

"ipaddress":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/systemrestorepoint/ filename_value<String>
Query-parameters: attrs http:// <netscaler-ip-address> /nitro/v1/config/systemrestorepoint/ filename_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/systemrestorepoint/ filename_value<String> ? **view=summary**

Use this query-parameter to get the summary output of systemrestorepoint resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "systemrestorepoint": [ {

"filename":<String_value>,

"backupfilename":<String_value>,

"techsuprtname":<String_value>,

"creationtime":<String_value>,

"version":<String_value>,

"createdby":<String_value>,

"ipaddress":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/systemrestorepoint? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "systemrestorepoint": [ { "__count": "#no"} ] }
```

systemsession

Configuration for system session resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
sid	<Integer>	Read-write	ID of the system session about which to display information. Minimum value = 1
all	<Boolean>	Read-write	Terminate all the system sessions except the current session.
username	<String>	Read-only	user name of the session.
logintime	<String>	Read-only	logged-in time of this session.
logintimelocal	<String>	Read-only	logged-in time (in local ADC timezone) of this session.
lastactivitytime	<String>	Read-only	last activity time of this session.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
lastactivitytimelocal	<String>	Read-only	last activity time (in local ADC timezone) of this session.
expirytime	<Integer>	Read-only	Time left in expire the session in seconds.
numofconnections	<Integer>	Read-only	number of connection using this token.
currentconn	<Boolean>	Read-only	True if the token is used for current session.
clienttype	<String>	Read-only	client type of the session. Possible values = CLI, CONSOLE, API, GUI
partitionname	<String>	Read-only	Name of the partition where the user is currently present.
clientipaddress	<String>	Read-only	IP address of client connecting to ADC.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET (ALL)
- GET
- COUNT

- KILL

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

KILL

URL: http:// <netscaler-ip-address> /nitro/v1/config/systemsession? **action=kill HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"systemsession":{

"sid":<Integer_value>,

"all":<Boolean_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/systemsession **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/systemsession? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/systemsession? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of systemsession resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/systemsession? **view=summary**

Use this query-parameter to get the summary output of systemsession resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/systemsession? **pagesize=#no;pageno=#no**

Use this query-parameter to get the systemsession resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "systemsession": [ {

"sid":<Integer_value>,

"username":<String_value>,

"logintime":<String_value>,

"logintimelocal":<String_value>,

"lastactivitytime":<String_value>,

"lastactivitytimelocal":<String_value>,

"expirytime":<Integer_value>,

"numofconnections":<Integer_value>,

"currentconn":<Boolean_value>,

"clienttype":<String_value>,

"partitionname":<String_value>,

"clientipaddress":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/systemsession/ sid_value<Integer> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/systemsession/ sid_value<Integer> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/systemsession/ sid_value<Integer> ? **view=summary**

Use this query-parameter to get the summary output of systemsession resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "systemsession": [ {

"sid":<Integer_value>,

"username":<String_value>,

"logintime":<String_value>,

"logintimelocal":<String_value>,
```

```
"lastactivitytime":<String_value>,

"lastactivitytimelocal":<String_value>,

"expirytime":<Integer_value>,

"numofconnections":<Integer_value>,

"currentconn":<Boolean_value>,

"clienttype":<String_value>,

"partitionname":<String_value>,

"clientipaddress":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/systemsession? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "systemsession": [ { "__count": "#no"} ] }
```

systemsignedexereport

Configuration for system signedExeReport resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
message	<String>	Read-write	.

Operations

(click to see Properties)

- ENABLE
- DISABLE

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ENABLE

URL: http:// <netscaler-ip-address> /nitro/v1/config/systemsignedexereport? **action=enable**

HTTP Method: POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"systemsignedexereport":{

}}
```

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DISABLE

URL: http:// <netscaler-ip-address> /nitro/v1/config/systemsignedexereport? **action=disable**

HTTP Method: POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"systemsignedexereport":{

}}
```

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

systemsshkey

Configuration for 0 resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	URL \(protocol, host, path, and file name\) from where the location file will be imported. NOTE: The import fails if the object to be imported is on an HTTPS server that requires client certificate authentication for access. Minimum length = 1 Maximum length = 255

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
sshkeytype	<String>	Read-write	The type of the ssh key whether public or private key. Possible values = PRIVATE, PUBLIC
src	<String>	Read-write	URL \(protocol, host, path, and file name\) from where the location file will be imported. NOTE: The import fails if the object to be imported is on an HTTPS server that requires client certificate authentication for access. Minimum length = 1 Maximum length = 2047
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- DELETE
- IMPORT
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/systemsshkey/ name_value<String> **Query-parameters: args= sshkeytype:<String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

IMPORT

URL: http:// <netscaler-ip-address> /nitro/v1/config/systemsshkey? **action=Import HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"systemsshkey":{

<b>"name":<String_value>,

</b><b>"src":<String_value>,

</b><b>"sshkeytype":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/systemsshkey **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/systemsshkey? **args=sshkeytype: <String_value>**

Use this query-parameter to get systemsshkey resources based on additional properties.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "systemsshkey": [ {

sshkeytype:<String_value>"name":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

systemuser

Configuration for system user resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
username	<String>	Read-write	Name for a user. Must begin with a letter, number, or the underscore (_) character, and must contain only alphanumeric, hyphen (-), period (.), hash (#), space ( ), at (@), equal (=), colon (:), and underscore characters. Cannot be changed after the user is added. CLI Users: If the name includes one or more spaces, enclose the name in double or single

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			quotation marks (for example, "my user" or 'my user'). Minimum length = 1
password	<String>	Read-write	Password for the system user. Can include any ASCII character. Minimum length = 1
externalauth	<String>	Read-write	Whether to use external authentication servers for the system user authentication or not. Default value: ENABLED Possible values = ENABLED, DISABLED
promptstring	<String>	Read-write	String to display at the command-line prompt. Can consist of letters, numbers, hyphen (-), period (.), hash (#), space ( ), at (@), equal (=), colon (:), underscore (_), and the following variables: * %u - Will be replaced by the user name.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			* %h - Will be replaced by the hostname of the Citrix ADC. * %t - Will be replaced by the current time in 12-hour format. * %T - Will be replaced by the current time in 24-hour format. * %d - Will be replaced by the current date. * %s - Will be replaced by the state of the Citrix ADC. Note: The 63-character limit for the length of the string does not apply to the characters that replace the variables. Minimum length = 1
timeout	<Integer>	Read-write	CLI session inactivity timeout, in seconds. If Restrictedtimeout argument of system

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			parameter is enabled, Timeout can have values in the range [300-86400] seconds. If Restrictedtimeout argument of system parameter is disabled, Timeout can have values in the range [0, 10-100000000] seconds. Default value is 900 seconds.
logging	<String>	Read-write	Users logging privilege. Default value: DISABLED Possible values = ENABLED, DISABLED
maxsession	<Integer>	Read-write	Maximum number of client connection allowed per user. Minimum value = 1 Maximum value = 40
allowedmanagementinterface	<String[]>	Read-write	Allowed Management interfaces to the system user. By default user is allowed from both API and CLI

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			interfaces. If management interface for a user is set to API, then user is not allowed to access NS through CLI. GUI interface will come under API interface. Default value: NS_INTERFACE_ALL Possible values = CLI, API
encrypted	<Boolean>	Read-only	.
hashmethod	<String>	Read-only	. Possible values = SHA1, SHA512, PBKDF2
promptinheritedfrom	<String>	Read-only	From where the prompt has been inherited. Possible values = User, Group, Global, Climode
timeoutkind	<String>	Read-only	From where the timeout has been inherited. Possible values = User, Group, Global, Climode
allowedmanagementinterfacekind	<String>	Read-only	Value of allowed interface which can be inherited from

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Global, Group or User. Possible values = User, Group, Global, Climode
lastpwdchangetimestamp	<Integer>	Read-only	Timestamp for the last password change for system user.
daystoexpirekind	<String>	Read-only	From where the daystoexpire value has been inherited. Possible values = User, Group, Global, Climode
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/systemuser **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"systemuser":{

<b>"username":<String_value>,

</b><b>"password":<String_value>,

</b>"externalauth":<String_value>,
```

```
"promptstring":<String_value>,

"timeout":<Integer_value>,

"logging":<String_value>,

"maxsession":<Integer_value>,

"allowedmanagementinterface":<String[]_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/systemuser/ username_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/systemuser **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"systemuser":{

<b>"username":<String_value>,

</b>"password":<String_value>,

"externalauth":<String_value>,

"promptstring":<String_value>,

"timeout":<Integer_value>,

"logging":<String_value>,

"maxsession":<Integer_value>,

"allowedmanagementinterface":<String[]_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/systemuser? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"systemuser":{

"allowedmanagementinterface":true,

<b>"username":<String_value>,
```

```
</b>"externalauth":true,

"promptstring":true,

"timeout":true,

"logging":true,

"maxsession":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/systemuser **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/systemuser? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/systemuser? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of systemuser resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/systemuser? **view=summary**

Use this query-parameter to get the summary output of systemuser resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/systemuser? **pagesize=#no;pageno=#no**

Use this query-parameter to get the systemuser resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "systemuser": [ {

"username":<String_value>,

"password":<String_value>,

"encrypted":<Boolean_value>,

"hashmethod":<String_value>,

"externalauth":<String_value>,

"promptstring":<String_value>,

"promptinheritedfrom":<String_value>,

"timeout":<Integer_value>,

"timeoutkind":<String_value>,

"logging":<String_value>,

"maxsession":<Integer_value>,

"allowedmanagementinterface":<String[]_value>,

"allowedmanagementinterfacekind":<String_value>,
```

```
"lastpwdchangetimestamp":<Integer_value>,

"daystoexpirekind":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/systemuser/ username_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/systemuser/ username_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/systemuser/ username_value<String> ? **view=summary**

Use this query-parameter to get the summary output of systemuser resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "systemuser": [ {

"username":<String_value>,

"password":<String_value>,

"encrypted":<Boolean_value>,

"hashmethod":<String_value>,

"externalauth":<String_value>,

"promptstring":<String_value>,

"promptinheritedfrom":<String_value>,

"timeout":<Integer_value>,

"timeoutkind":<String_value>,

"logging":<String_value>,

"maxsession":<Integer_value>,

"allowedmanagementinterface":<String[]_value>,

"allowedmanagementinterfacekind":<String_value>,

"lastpwdchangetimestamp":<Integer_value>,

"daystoexpirekind":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/systemuser? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "systemuser": [ { "__count": "#no"} ] }
```

systemuser_binding

Binding object which returns the resources bound to systemuser.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
username	<String>	Read-write	Name of a system user about whom to display information. Minimum length = 1
systemuser_nspartition_binding	<systemuser_nspartition_binding[]>	Read-only	nspartition that can be bound to systemuser.
systemuser_systemgroup_binding	<systemuser_systemgroup_binding[]>	Read-only	systemgroup that can be bound to systemuser.
systemuser_systemcmdpolicy_binding	<systemuser_systemcmdpolicy_binding[]>	Read-only	systemcmdpolicy that can be bound to systemuser.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/systemuser_binding/ username_value<String>
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "systemuser_binding": [ {

"username":<String_value>,

"systemuser_systemcmdpolicy_binding":<systemuser_systemcmdpolicy_binding[]
_value>,

"systemuser_nspartition_binding":<systemuser_nspartition_binding[]_value>,

"systemuser_systemgroup_binding":<systemuser_systemgroup_binding[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/systemuser_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/systemuser_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "systemuser_binding": [ {

"username":<String_value>,

"systemuser_systemcmdpolicy_binding":<systemuser_systemcmdpolicy_binding[]
_value>,

"systemuser_nspartition_binding":<systemuser_nspartition_binding[]_value>,

"systemuser_systemgroup_binding":<systemuser_systemgroup_binding[]_value>

}]}
```

systemuser_nspartition_binding

Binding object showing the nspartition that can be bound to systemuser.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
username	<String>	Read-write	Name of the system-user entry to which to bind the command policy. Minimum length = 1
partitionname	<String>	Read-write	Name of the Partition to bind to the system user.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/systemuser_nspartition_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"systemuser_nspartition_binding":{

<b>"username":<String_value>,

</b>"partitionname":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/systemuser_nspartition_binding/ username_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ systemuser_nspartition_binding/ username_value<String> ? **args=partitionname: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/systemuser_nspartition_binding/ username_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ systemuser_nspartition_binding/ username_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of systemuser_nspartition_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/systemuser_nspartition_binding/ username_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the systemuser_nspartition_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "systemuser_nspartition_binding": [ {

"username":<String_value>,

"partitionname":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/systemuser_nspartition_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/systemuser_nspartition_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "systemuser_nspartition_binding": [ {

"username":<String_value>,

"partitionname":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/systemuser_nspartition_binding/username_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"systemuser_nspartition_binding": [ { "__count": "#no"} ] }
```

systemuser_systemcmdpolicy_binding

Binding object showing the systemcmdpolicy that can be bound to systemuser.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
priority	<Integer>	Read-write	The priority of the policy.
policyname	<String>	Read-write	The name of command policy.
username	<String>	Read-write	Name of the system-user entry to which to bind the command policy. Minimum length = 1
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/systemuser_systemcmdpolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"systemuser_systemcmdpolicy_binding":{

<b>"username":<String_value>,

</b>"policyname":<String_value>,

"priority":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/systemuser_systemcmdpolicy_binding/ username_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ systemuser_systemcmdpolicy_binding/ username_value<String> ? **args=policyname: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/systemuser_systemcmdpolicy_binding/ username_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ systemuser_systemcmdpolicy_binding/ username_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of systemuser_systemcmdpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/systemuser_systemcmdpolicy_binding/ username_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the systemuser_systemcmdpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "systemuser_systemcmdpolicy_binding": [ {

"priority":<Integer_value>,

"policyname":<String_value>,

"username":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/systemuser_systemcmdpolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/systemuser_systemcmdpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "systemuser_systemcmdpolicy_binding": [ {

"priority":<Integer_value>,

"policyname":<String_value>,

"username":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/systemuser_systemcmdpolicy_binding/username_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"systemuser_systemcmdpolicy_binding": [ { "__count": "#no"} ] }
```

systemuser_systemgroup_binding

Binding object showing the systemgroup that can be bound to systemuser.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
groupname	<String>	Read-write	The system group. .
username	<String>	Read-write	Name of the system-user entry to which to bind the command policy. Minimum length = 1
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)

- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/systemuser_systemgroup_binding/ username_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ systemuser_systemgroup_binding/ username_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of systemuser_systemgroup_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/systemuser_systemgroup_binding/ username_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the systemuser_systemgroup_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "systemuser_systemgroup_binding": [ {

"groupname":<String_value>,

"username":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/systemuser_systemgroup_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/systemuser_systemgroup_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "systemuser_systemgroup_binding": [ {

"groupname":<String_value>,

"username":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/systemuser_systemgroup_binding/ username_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"systemuser_systemgroup_binding": [ { "__count": "#no"} ] }
```

tm

Traffic Management

TM session/policy configuration.

NAME	DESCRIPTION
tmformssoaction	Configuration for Form sso action
tmglobal_auditnslogpolicy_binding	Binding object showing the auditnslogpolicy that can be bound to tmglobal
tmglobal_auditsyslogpolicy_binding	Binding object showing the auditsyslogpolicy that can be bound to tmglobal
tmglobal_binding	Binding object showing the resources that can be bound to tmglobal
tmglobal_tmsessionpolicy_binding	Binding object showing the tmsessionpolicy that can be bound to tmglobal
tmglobal_tmtrafficpolicy_binding	Binding object showing the tmtrafficpolicy that can be bound to tmglobal
tmsamlssoprofile	Configuration for SAML sso action
tmsessionaction	Configuration for TM session action
tmsessionparameter	Configuration for session parameter
tmsessionpolicy	Configuration for TM session policy

NAME	DESCRIPTION
tmsessionpolicy_aaagroup_binding	Binding object showing the aaagroup that can be bound to tmsessionpolicy
tmsessionpolicy_aaauser_binding	Binding object showing the aaauser that can be bound to tmsessionpolicy
tmsessionpolicy_authenticationvserver_binding	Binding object showing the authenticationvserver that can be bound to tmsessionpolicy
tmsessionpolicy_binding	Binding object showing the resources that can be bound to tmsessionpolicy
tmsessionpolicy_tmglobal_binding	Binding object showing the tmglobal that can be bound to tmsessionpolicy
tmtrafficaction	Configuration for TM traffic action
tmtrafficpolicy	Configuration for TM traffic policy
tmtrafficpolicy_binding	Binding object showing the resources that can be bound to tmtrafficpolicy
tmtrafficpolicy_csvserver_binding	Binding object showing the csvserver that can be bound to tmtrafficpolicy
tmtrafficpolicy_lbvserver_binding	Binding object showing the lbvserver that can be bound to tmtrafficpolicy
tmtrafficpolicy_tmglobal_binding	Binding object showing the tmglobal that can be bound to tmtrafficpolicy

NAME	DESCRIPTION

tmformssoaction

Configuration for Form sso action resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the new form-based single sign-on profile. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after an SSO action is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			"my action" or 'my action'). Minimum length = 1
actionurl	<String>	Read-write	URL to which the completed form is submitted. Minimum length = 1
userfield	<String>	Read-write	Name of the form field in which the user types in the user ID. Minimum length = 1
passwdfield	<String>	Read-write	Name of the form field in which the user types in the password. Minimum length = 1
ssosuccessrule	<String>	Read-write	Expression, that checks to see if single sign-on is successful.
namevaluepair	<String>	Read-write	Name-value pair attributes to send to the server in addition to sending the username and password. Value names are separated by an ampersand (;) (for example, name1=value1;name2=value2).
responsesize	<Integer>	Read-write	Number of bytes, in the response, to

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			parse for extracting the forms. Default value: 8096
nvtype	<String>	Read-write	Type of processing of the name-value pair. If you specify STATIC, the values configured by the administrator are used. For DYNAMIC, the response is parsed, and the form is extracted and then submitted. Default value: DYNAMIC Possible values = STATIC, DYNAMIC
submitmethod	<String>	Read-write	HTTP method used by the single sign-on form to send the logon credentials to the logon server. Applies only to STATIC name-value type. Default value: GET Possible values = GET, POST
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/tmformssoaction **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"tmformssoaction":{

<b>"name":<String_value>,

</b><b>"actionurl":<String_value>,

</b><b>"userfield":<String_value>,

</b><b>"passwdfield":<String_value>,

</b><b>"ssosuccessrule":<String_value>,

</b>"namevaluepair":<String_value>,

"responsesize":<Integer_value>,

"nvtype":<String_value>,

"submitmethod":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/tmformssoaction/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/tmformssoaction **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"tmformssoaction":{

<b>"name":<String_value>,

</b>"actionurl":<String_value>,

"userfield":<String_value>,

"passwdfield":<String_value>,

"ssosuccessrule":<String_value>,

"responsesize":<Integer_value>,

"namevaluepair":<String_value>,

"nvtype":<String_value>,

"submitmethod":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/tmformssoaction? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"tmformssoaction":{

<b>"name":<String_value>,

</b>"responsesize":true,

"namevaluepair":true,

"nvtype":true,

"submitmethod":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/tmformssoaction **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/tmformssoaction? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/tmformssoaction? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of tmformssoaction resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/tmformssoaction? **view=summary**

Use this query-parameter to get the summary output of tmformssoaction resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/tmformssoaction? **pagesize=#no;pageno=#no**

Use this query-parameter to get the tmformssoaction resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "tmformssoaction": [ {

"name":<String_value>,

"actionurl":<String_value>,

"userfield":<String_value>,

"passwdfield":<String_value>,

"responsesize":<Integer_value>,
```

```
"namevaluepair":<String_value>,

"nvtype":<String_value>,

"ssosuccessrule":<String_value>,

"submitmethod":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/tmformssoaction/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/tmformssoaction/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/tmformssoaction/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of tmformssoaction resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "tmformssoaction": [ {

"name":<String_value>,

"actionurl":<String_value>,

"userfield":<String_value>,

"passwdfield":<String_value>,

"responsesize":<Integer_value>,

"namevaluepair":<String_value>,

"nvtype":<String_value>,

"ssosuccessrule":<String_value>,

"submitmethod":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/tmformssoaction? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "tmformssoaction": [ { "__count": "#no"} ] }
```

tmglobal_auditnslogpolicy_binding

Binding object showing the auditnslogpolicy that can be bound to tmglobal.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
gotopriorityexpression	<String>	Read-write	Applicable only to advance tmsession policy. Expression or other value specifying the next policy to be evaluated if the current policy evaluates to TRUE. Specify one of the following values: * NEXT - Evaluate the policy with the next higher priority number. * END - End policy evaluation. * An expression that evaluates to a number. If you specify an expression, the number to which it evaluates determines the next policy to evaluate, as

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			follows: * If the expression evaluates to a higher numbered priority, the policy with that priority is evaluated next. * If the expression evaluates to the priority of the current policy, the policy with the next higher numbered priority is evaluated next. * If the expression evaluates to a priority number that is numerically higher than the highest numbered priority, policy evaluation ends. An UNDEF event is triggered if: * The expression is invalid. * The expression evaluates to a priority number that is numerically lower than the current policy's priority. * The expression evaluates to a priority number that is between the current policy's priority number (say, 30) and the highest priority number (say, 100), but does not match any configured priority number (for

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			example, the expression evaluates to the number 85). This example assumes that the priority number increments by 10 for every successive policy, and therefore a priority number of 85 does not exist in the policy label.
priority	<Integer>	Read-write	The priority of the policy.
policyname	<String>	Read-write	The name of the policy.
priority	<Integer>	Read-write	The priority of the policy.
bindpolicytype	<Integer>	Read-only	Bound policy type.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/tmglobal_auditnslogpolicy_binding

HTTP Method: PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"tmglobal_auditnslogpolicy_binding":{

"policyname":<String_value>,

"priority":<Integer_value>,

"gotopriorityexpression":<String_value>
```

```
}}
```

Response:

HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/tmglobal_auditnslogpolicy_binding

Query-parameters:

args

http:// <netscaler-ip-address> /nitro/v1/config/tmglobal_auditnslogpolicy_binding? **args=policyname: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/tmglobal_auditnslogpolicy_binding

Query-parameters:

filter

http:// <netscaler-ip-address> /nitro/v1/config/tmglobal_auditnslogpolicy_binding? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of tmglobal_auditnslogpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination

http:// <netscaler-ip-address> /nitro/v1/config/tmglobal_auditnslogpolicy_binding?
pagesize=#no;pageno=#no

Use this query-parameter to get the tmglobal_auditnslogpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "tmglobal_auditnslogpolicy_binding": [ {

"gotopriorityexpression":<String_value>,

"priority":<Integer_value>,

"policyname":<String_value>,

"priority":<Integer_value>,

"bindpolicytype":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/tmglobal_auditnslogpolicy_binding? **count=yes**

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "tmglobal_auditnslogpolicy_binding": [ { "__count": "#no"} ] }
```

tmglobal_auditsyslogpolicy_binding

Binding object showing the auditsyslogpolicy that can be bound to tmglobal.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
policyname	<String>	Read-write	The name of the policy.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
priority	<Integer>	Read-write	The priority of the policy.
gotopriorityexpression	<String>	Read-write	Applicable only to advance tmsession policy. Expression or other value specifying the next policy to be evaluated if the current policy evaluates to TRUE. Specify one of the following values: * NEXT - Evaluate the policy with the next higher priority number. * END - End policy evaluation. * An expression that evaluates to a number. If you specify an expression, the number to which it evaluates determines the next policy to evaluate, as follows: * If the expression evaluates to a higher numbered priority, the policy with that priority is evaluated next. * If the expression evaluates to the priority of the current policy, the policy with the next higher numbered priority is evaluated

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			next. * If the expression evaluates to a priority number that is numerically higher than the highest numbered priority, policy evaluation ends. An UNDEF event is triggered if: * The expression is invalid. * The expression evaluates to a priority number that is numerically lower than the current policy's priority. * The expression evaluates to a priority number that is between the current policy's priority number (say, 30) and the highest priority number (say, 100), but does not match any configured priority number (for example, the expression evaluates to the number 85). This example assumes that the priority number increments by 10 for every successive policy, and therefore a priority number of 85 does not exist in the policy label.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
bindpolicytype	<Integer>	Read-only	Bound policy type.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/tmglobal_auditsyslogpolicy_binding

HTTP Method: PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"tmglobal_auditsyslogpolicy_binding":{

"policyname":<String_value>,

"priority":<Integer_value>,

"gotopriorityexpression":<String_value>

}}
```

Response:

HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/tmglobal_auditsyslogpolicy_binding

Query-parameters:

args

http:// <netscaler-ip-address> /nitro/v1/config/tmglobal_auditsyslogpolicy_binding?
args=policyname: <String_value>

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/tmglobal_auditsyslogpolicy_binding

Query-parameters:

filter

http:// <netscaler-ip-address> /nitro/v1/config/tmglobal_auditsyslogpolicy_binding? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of tmglobal_auditsyslogpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination

http:// <netscaler-ip-address> /nitro/v1/config/tmglobal_auditsyslogpolicy_binding? **pagesize=#no;pageno=#no**

Use this query-parameter to get the tmglobal_auditsyslogpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "tmglobal_auditsyslogpolicy_binding": [ {

"policyname":<String_value>,

"priority":<Integer_value>,

"gotopriorityexpression":<String_value>,

"bindpolicytype":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/tmglobal_auditsyslogpolicy_binding?**count=yes**

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "tmglobal_auditsyslogpolicy_binding": [ { "__count": "#no"} ] }
```

tmglobal_binding

Binding object which returns the resources bound to tmglobal.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
tmglobal_auditsyslogpolicy_binding	<tmglobal_auditsyslogpolicy_binding[]>	Read-write	auditsyslogpolicy that can be bound to tmglobal.
tmglobal_tmsessionpolicy_binding	<tmglobal_tmsessionpolicy_binding[]>	Read-write	tmsessionpolicy that can be bound to tmglobal.
tmglobal_tmtrafficpolicy_binding	<tmglobal_tmtrafficpolicy_binding[]>	Read-write	tmtrafficpolicy that can be bound to tmglobal.
tmglobal_auditnslogpolicy_binding	<tmglobal_auditnslogpolicy_binding[]>	Read-write	auditnslogpolicy that can be bound to tmglobal.

Operations

(click to see Properties)

- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/tmglobal_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "tmglobal_binding": [ {

"tmglobal_tmtrafficpolicy_binding":<tmglobal_tmtrafficpolicy_binding[]_value>,

"tmglobal_auditsyslogpolicy_binding":<tmglobal_auditsyslogpolicy_binding[]_value>,

"tmglobal_auditnslogpolicy_binding":<tmglobal_auditnslogpolicy_binding[]_value>,

"tmglobal_tmsessionpolicy_binding":<tmglobal_tmsessionpolicy_binding[]_value>

}]}
```

tmglobal_tmsessionpolicy_binding

Binding object showing the tmsessionpolicy that can be bound to tmglobal.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
priority	<Integer>	Read-write	The priority of the policy.
builtin	<String[]>	Read-write	Indicates that a variable is a built-in (SYSTEM INTERNAL) type. Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
feature	<String>	Read-write	The feature to be checked while applying this config.
gotopriorityexpression	<String>	Read-write	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
policyname	<String>	Read-write	The name of the policy.
bindpolicytype	<Integer>	Read-only	Bound policy type.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/tmglobal_tmsessionpolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"tmglobal_tmsessionpolicy_binding":{

"policyname":<String_value>,

"priority":<Integer_value>,

"gotopriorityexpression":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/tmglobal_tmsessionpolicy_binding **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/tmglobal_tmsessionpolicy_binding? **args=policyname: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/tmglobal_tmsessionpolicy_binding **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/tmglobal_tmsessionpolicy_binding? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of tmglobal_tmsessionpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/tmglobal_tmsessionpolicy_binding? **pagesize=#no;pageno=#no**

Use this query-parameter to get the tmglobal_tmsessionpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "tmglobal_tmsessionpolicy_binding": [ {

"priority":<Integer_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"gotopriorityexpression":<String_value>,

"policyname":<String_value>,

"bindpolicytype":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/tmglobal_tmsessionpolicy_binding? **count=yes**
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "tmglobal_tmsessionpolicy_binding": [ { "__count": "#no"} ] }
```

tmglobal_tmtrafficpolicy_binding

Binding object showing the tmtrafficpolicy that can be bound to tmglobal.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
priority	<Integer>	Read-write	The priority of the policy.
policyname	<String>	Read-write	The name of the policy.
globalbindtype	<String>	Read-write	. Default value: SYSTEM_GLOBAL Possible values = SYSTEM_GLOBAL, VPN_GLOBAL, RNAT_GLOBAL, APPFW_GLOBAL, TM_GLOBAL
gotopriorityexpression	<String>	Read-write	Applicable only to advance tmsession policy. Expression or other value specifying the next policy to be evaluated if the current policy evaluates to TRUE. Specify one of the following values: *

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			NEXT - Evaluate the policy with the next higher priority number. * END - End policy evaluation. * An expression that evaluates to a number. If you specify an expression, the number to which it evaluates determines the next policy to evaluate, as follows: * If the expression evaluates to a higher numbered priority, the policy with that priority is evaluated next. * If the expression evaluates to the priority of the current policy, the policy with the next higher numbered priority is evaluated next. * If the expression evaluates to a priority number that is numerically higher than the highest numbered priority, policy evaluation ends. An UNDEF event is triggered if: * The expression is invalid. * The expression evaluates to a priority number that

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			is numerically lower than the current policy's priority. * The expression evaluates to a priority number that is between the current policy's priority number (say, 30) and the highest priority number (say, 100), but does not match any configured priority number (for example, the expression evaluates to the number 85). This example assumes that the priority number increments by 10 for every successive policy, and therefore a priority number of 85 does not exist in the policy label.
type	<String>	Read-write	Bindpoint to which the policy is bound. Possible values = REQ_OVERRIDE, REQ_DEFAULT, RES_OVERRIDE, RES_DEFAULT
bindpolicytype	<Integer>	Read-only	Bound policy type.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/tmglobal_tmtrafficpolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"tmglobal_tmtrafficpolicy_binding":{

"policyname":<String_value>,

"priority":<Integer_value>,

"gotopriorityexpression":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/tmglobal_tmtrafficpolicy_binding **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/tmglobal_tmtrafficpolicy_binding?**args=policyname: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/tmglobal_tmtrafficpolicy_binding **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/tmglobal_tmtrafficpolicy_binding?**filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of tmglobal_tmtrafficpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/tmglobal_tmtrafficpolicy_binding?**pagesize=#no;pageno=#no**

Use this query-parameter to get the tmglobal_tmtrafficpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "tmglobal_tmtrafficpolicy_binding": [ {

"priority":<Integer_value>,

"policyname":<String_value>,

"globalbindtype":<String_value>,

"gotopriorityexpression":<String_value>,

"type":<String_value>,
```

```
"bindpolicytype":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/tmglobal_tmtrafficpolicy_binding? **count=yes**
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "tmglobal_tmtrafficpolicy_binding": [ { "__count": "#no"} ] }
```

tmsamlssoprofile

Configuration for SAML sso action resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the new saml single sign-on profile. Must begin with an ASCII

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after an SSO action is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my action" or 'my action'). Minimum length = 1
samlsigningcertname	<String>	Read-write	Name of the SSL certificate that is used to Sign Assertion. Minimum length = 1
assertionconsumerserviceurl	<String>	Read-write	URL to which the assertion is to be sent.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum length = 1
relaystaterule	<String>	Read-write	Expression to extract relaystate to be sent along with assertion. Evaluation of this expression should return TEXT content. This is typically a targ et url to which user is redirected after the recipient validates SAML token.
sendpassword	<String>	Read-write	Option to send password in assertion. Default value: OFF Possible values = ON, OFF
samlissuername	<String>	Read-write	The name to be used in requests sent from Citrix ADC to IdP to uniquely identify Citrix ADC. Minimum length = 1
signaturealg	<String>	Read-write	Algorithm to be used to sign/verify SAML transactions. Default value: RSA-SHA256

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = RSA-SHA1, RSA-SHA256
digestmethod	<String>	Read-write	Algorithm to be used to compute/verify digest for SAML transactions. Default value: SHA256 Possible values = SHA1, SHA256
audience	<String>	Read-write	Audience for which assertion sent by IdP is applicable. This is typically entity name or url that represents ServiceProvider.
nameidformat	<String>	Read-write	Format of Name Identifier sent in Assertion. Default value: transient Possible values = Unspecified, emailAddress, X509SubjectName, WindowsDomainQualifiedName, kerberos, entity, persistent, transient
nameidexpr	<String>	Read-write	Expression that will be evaluated to obtain

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			NameIdentifier to be sent in assertion. Maximum length = 128
attribute1	<String>	Read-write	Name of attribute1 that needs to be sent in SAML Assertion.
attribute1expr	<String>	Read-write	Expression that will be evaluated to obtain attribute1's value to be sent in Assertion. Maximum length = 128
attribute1friendlyname	<String>	Read-write	User-Friendly Name of attribute1 that needs to be sent in SAML Assertion.
attribute1format	<String>	Read-write	Format of Attribute1 to be sent in Assertion. Possible values = URI, Basic
attribute2	<String>	Read-write	Name of attribute2 that needs to be sent in SAML Assertion.
attribute2expr	<String>	Read-write	Expression that will be evaluated to obtain attribute2's value to be sent in Assertion. Maximum length = 128

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
attribute2friendlyname	<String>	Read-write	User-Friendly Name of attribute2 that needs to be sent in SAML Assertion.
attribute2format	<String>	Read-write	Format of Attribute2 to be sent in Assertion. Possible values = URI, Basic
attribute3	<String>	Read-write	Name of attribute3 that needs to be sent in SAML Assertion.
attribute3expr	<String>	Read-write	Expression that will be evaluated to obtain attribute3's value to be sent in Assertion. Maximum length = 128
attribute3friendlyname	<String>	Read-write	User-Friendly Name of attribute3 that needs to be sent in SAML Assertion.
attribute3format	<String>	Read-write	Format of Attribute3 to be sent in Assertion. Possible values = URI, Basic
attribute4	<String>	Read-write	Name of attribute4 that needs to be sent in SAML Assertion.
attribute4expr	<String>	Read-write	Expression that will be evaluated to

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			obtain attribute4's value to be sent in Assertion. Maximum length = 128
attribute4friendlyname	<String>	Read-write	User-Friendly Name of attribute4 that needs to be sent in SAML Assertion.
attribute4format	<String>	Read-write	Format of Attribute4 to be sent in Assertion. Possible values = URI, Basic
attribute5	<String>	Read-write	Name of attribute5 that needs to be sent in SAML Assertion.
attribute5expr	<String>	Read-write	Expression that will be evaluated to obtain attribute5's value to be sent in Assertion. Maximum length = 128
attribute5friendlyname	<String>	Read-write	User-Friendly Name of attribute5 that needs to be sent in SAML Assertion.
attribute5format	<String>	Read-write	Format of Attribute5 to be sent in Assertion. Possible values = URI, Basic

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
attribute6	<String>	Read-write	Name of attribute6 that needs to be sent in SAML Assertion.
attribute6expr	<String>	Read-write	Expression that will be evaluated to obtain attribute6's value to be sent in Assertion. Maximum length = 128
attribute6friendlyname	<String>	Read-write	User-Friendly Name of attribute6 that needs to be sent in SAML Assertion.
attribute6format	<String>	Read-write	Format of Attribute6 to be sent in Assertion. Possible values = URI, Basic
attribute7	<String>	Read-write	Name of attribute7 that needs to be sent in SAML Assertion.
attribute7expr	<String>	Read-write	Expression that will be evaluated to obtain attribute7's value to be sent in Assertion. Maximum length = 128
attribute7friendlyname	<String>	Read-write	User-Friendly Name of attribute7 that needs to be sent in SAML Assertion.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
attribute7format	<String>	Read-write	Format of Attribute7 to be sent in Assertion. Possible values = URI, Basic
attribute8	<String>	Read-write	Name of attribute8 that needs to be sent in SAML Assertion.
attribute8expr	<String>	Read-write	Expression that will be evaluated to obtain attribute8's value to be sent in Assertion. Maximum length = 128
attribute8friendlyname	<String>	Read-write	User-Friendly Name of attribute8 that needs to be sent in SAML Assertion.
attribute8format	<String>	Read-write	Format of Attribute8 to be sent in Assertion. Possible values = URI, Basic
attribute9	<String>	Read-write	Name of attribute9 that needs to be sent in SAML Assertion.
attribute9expr	<String>	Read-write	Expression that will be evaluated to obtain attribute9's value to be sent in Assertion. Maximum length = 128

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
attribute9friendlyname	<String>	Read-write	User-Friendly Name of attribute9 that needs to be sent in SAML Assertion.
attribute9format	<String>	Read-write	Format of Attribute9 to be sent in Assertion. Possible values = URI, Basic
attribute10	<String>	Read-write	Name of attribute10 that needs to be sent in SAML Assertion.
attribute10expr	<String>	Read-write	Expression that will be evaluated to obtain attribute10's value to be sent in Assertion. Maximum length = 128
attribute10friendlyname	<String>	Read-write	User-Friendly Name of attribute10 that needs to be sent in SAML Assertion.
attribute10format	<String>	Read-write	Format of Attribute10 to be sent in Assertion. Possible values = URI, Basic
attribute11	<String>	Read-write	Name of attribute11 that needs to be sent in SAML Assertion.
attribute11expr	<String>	Read-write	Expression that will be evaluated to

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			obtain attribute11's value to be sent in Assertion. Maximum length = 128
attribute11friendlyname	<String>	Read-write	User-Friendly Name of attribute11 that needs to be sent in SAML Assertion.
attribute11format	<String>	Read-write	Format of Attribute11 to be sent in Assertion. Possible values = URI, Basic
attribute12	<String>	Read-write	Name of attribute12 that needs to be sent in SAML Assertion.
attribute12expr	<String>	Read-write	Expression that will be evaluated to obtain attribute12's value to be sent in Assertion. Maximum length = 128
attribute12friendlyname	<String>	Read-write	User-Friendly Name of attribute12 that needs to be sent in SAML Assertion.
attribute12format	<String>	Read-write	Format of Attribute12 to be sent in Assertion. Possible values = URI, Basic

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
attribute13	<String>	Read-write	Name of attribute13 that needs to be sent in SAML Assertion.
attribute13expr	<String>	Read-write	Expression that will be evaluated to obtain attribute13's value to be sent in Assertion. Maximum length = 128
attribute13friendlyname	<String>	Read-write	User-Friendly Name of attribute13 that needs to be sent in SAML Assertion.
attribute13format	<String>	Read-write	Format of Attribute13 to be sent in Assertion. Possible values = URI, Basic
attribute14	<String>	Read-write	Name of attribute14 that needs to be sent in SAML Assertion.
attribute14expr	<String>	Read-write	Expression that will be evaluated to obtain attribute14's value to be sent in Assertion. Maximum length = 128
attribute14friendlyname	<String>	Read-write	User-Friendly Name of attribute14 that needs to be sent in SAML Assertion.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
attribute14format	<String>	Read-write	Format of Attribute14 to be sent in Assertion. Possible values = URI, Basic
attribute15	<String>	Read-write	Name of attribute15 that needs to be sent in SAML Assertion.
attribute15expr	<String>	Read-write	Expression that will be evaluated to obtain attribute15's value to be sent in Assertion. Maximum length = 128
attribute15friendlyname	<String>	Read-write	User-Friendly Name of attribute15 that needs to be sent in SAML Assertion.
attribute15format	<String>	Read-write	Format of Attribute15 to be sent in Assertion. Possible values = URI, Basic
attribute16	<String>	Read-write	Name of attribute16 that needs to be sent in SAML Assertion.
attribute16expr	<String>	Read-write	Expression that will be evaluated to obtain attribute16's value to be sent in Assertion. Maximum length = 128

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
attribute16friendlyname	<String>	Read-write	User-Friendly Name of attribute16 that needs to be sent in SAML Assertion.
attribute16format	<String>	Read-write	Format of Attribute16 to be sent in Assertion. Possible values = URI, Basic
encryptassertion	<String>	Read-write	Option to encrypt assertion when Citrix ADC sends one. Default value: OFF Possible values = ON, OFF
samlspcertname	<String>	Read-write	Name of the SSL certificate of peer/ receving party using which Assertion is encrypted. Minimum length = 1
encryptionalgorithm	<String>	Read-write	Algorithm to be used to encrypt SAML assertion. Default value: AES256 Possible values = DES3, AES128, AES192, AES256
skewtime	<Integer>	Read-write	This option specifies the number of minutes on either side of current time

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			that the assertion would be valid. For example, if skewTime is 10, then assertion would be valid from (current time - 10) min to (current time + 10) min, ie 20min in all. Default value: 5
signassertion	<String>	Read-write	Option to sign portions of assertion when Citrix ADC IDP sends one. Based on the user selection, either Assertion or Response or Both or none can be signed. Default value: ASSERTION Possible values = NONE, ASSERTION, RESPONSE, BOTH
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET

- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/tmsamlssoprofile **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"tmsamlssoprofile":{

<b>"name":<String_value>,

</b>"samlsigningcertname":<String_value>,

<b>"assertionconsumerserviceurl":<String_value>,

</b>"relaystaterule":<String_value>,

"sendpassword":<String_value>,

"samlissuername":<String_value>,

"signaturealg":<String_value>,

"digestmethod":<String_value>,

"audience":<String_value>,

"nameidformat":<String_value>,

"nameidexpr":<String_value>,

"attribute1":<String_value>,

"attribute1expr":<String_value>,

"attribute1friendlyname":<String_value>,

"attribute1format":<String_value>,

"attribute2":<String_value>,

"attribute2expr":<String_value>,

"attribute2friendlyname":<String_value>,

"attribute2format":<String_value>,

"attribute3":<String_value>,

"attribute3expr":<String_value>,
```

```
"attribute3friendlyname":<String_value>,

"attribute3format":<String_value>,

"attribute4":<String_value>,

"attribute4expr":<String_value>,

"attribute4friendlyname":<String_value>,

"attribute4format":<String_value>,

"attribute5":<String_value>,

"attribute5expr":<String_value>,

"attribute5friendlyname":<String_value>,

"attribute5format":<String_value>,

"attribute6":<String_value>,

"attribute6expr":<String_value>,

"attribute6friendlyname":<String_value>,

"attribute6format":<String_value>,

"attribute7":<String_value>,

"attribute7expr":<String_value>,

"attribute7friendlyname":<String_value>,

"attribute7format":<String_value>,

"attribute8":<String_value>,

"attribute8expr":<String_value>,

"attribute8friendlyname":<String_value>,

"attribute8format":<String_value>,
```

```
"attribute9":<String_value>,

"attribute9expr":<String_value>,

"attribute9friendlyname":<String_value>,

"attribute9format":<String_value>,

"attribute10":<String_value>,

"attribute10expr":<String_value>,

"attribute10friendlyname":<String_value>,

"attribute10format":<String_value>,

"attribute11":<String_value>,

"attribute11expr":<String_value>,

"attribute11friendlyname":<String_value>,

"attribute11format":<String_value>,

"attribute12":<String_value>,

"attribute12expr":<String_value>,

"attribute12friendlyname":<String_value>,

"attribute12format":<String_value>,

"attribute13":<String_value>,

"attribute13expr":<String_value>,

"attribute13friendlyname":<String_value>,

"attribute13format":<String_value>,

"attribute14":<String_value>,

"attribute14expr":<String_value>,
```

```
"attribute14friendlyname":<String_value>,

"attribute14format":<String_value>,

"attribute15":<String_value>,

"attribute15expr":<String_value>,

"attribute15friendlyname":<String_value>,

"attribute15format":<String_value>,

"attribute16":<String_value>,

"attribute16expr":<String_value>,

"attribute16friendlyname":<String_value>,

"attribute16format":<String_value>,

"encryptassertion":<String_value>,

"samlspcertname":<String_value>,

"encryptionalgorithm":<String_value>,

"skewtime":<Integer_value>,

"signassertion":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/tmsamlssoprofile/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/tmsamlssoprofile **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"tmsamlssoprofile":{

<b>"name":<String_value>,

</b>"samlsigningcertname":<String_value>,

"assertionconsumerserviceurl":<String_value>,

"sendpassword":<String_value>,

"samlissuername":<String_value>,

"relaystaterule":<String_value>,

"signaturealg":<String_value>,

"digestmethod":<String_value>,

"audience":<String_value>,

"nameidformat":<String_value>,

"nameidexpr":<String_value>,
```

```
"attribute1":<String_value>,

"attribute1expr":<String_value>,

"attribute1friendlyname":<String_value>,

"attribute1format":<String_value>,

"attribute2":<String_value>,

"attribute2expr":<String_value>,

"attribute2friendlyname":<String_value>,

"attribute2format":<String_value>,

"attribute3":<String_value>,

"attribute3expr":<String_value>,

"attribute3friendlyname":<String_value>,

"attribute3format":<String_value>,

"attribute4":<String_value>,

"attribute4expr":<String_value>,

"attribute4friendlyname":<String_value>,

"attribute4format":<String_value>,

"attribute5":<String_value>,

"attribute5expr":<String_value>,

"attribute5friendlyname":<String_value>,

"attribute5format":<String_value>,

"attribute6":<String_value>,

"attribute6expr":<String_value>,
```

```
"attribute6friendlyname":<String_value>,

"attribute6format":<String_value>,

"attribute7":<String_value>,

"attribute7expr":<String_value>,

"attribute7friendlyname":<String_value>,

"attribute7format":<String_value>,

"attribute8":<String_value>,

"attribute8expr":<String_value>,

"attribute8friendlyname":<String_value>,

"attribute8format":<String_value>,

"attribute9":<String_value>,

"attribute9expr":<String_value>,

"attribute9friendlyname":<String_value>,

"attribute9format":<String_value>,

"attribute10":<String_value>,

"attribute10expr":<String_value>,

"attribute10friendlyname":<String_value>,

"attribute10format":<String_value>,

"attribute11":<String_value>,

"attribute11expr":<String_value>,

"attribute11friendlyname":<String_value>,

"attribute11format":<String_value>,
```

```
"attribute12":<String_value>,

"attribute12expr":<String_value>,

"attribute12friendlyname":<String_value>,

"attribute12format":<String_value>,

"attribute13":<String_value>,

"attribute13expr":<String_value>,

"attribute13friendlyname":<String_value>,

"attribute13format":<String_value>,

"attribute14":<String_value>,

"attribute14expr":<String_value>,

"attribute14friendlyname":<String_value>,

"attribute14format":<String_value>,

"attribute15":<String_value>,

"attribute15expr":<String_value>,

"attribute15friendlyname":<String_value>,

"attribute15format":<String_value>,

"attribute16":<String_value>,

"attribute16expr":<String_value>,

"attribute16friendlyname":<String_value>,

"attribute16format":<String_value>,

"encryptassertion":<String_value>,

"samlspcertname":<String_value>,
```

```
"encryptionalgorithm":<String_value>,

"skewtime":<Integer_value>,

"signassertion":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/tmsamlssoprofile? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"tmsamlssoprofile":{

<b>"name":<String_value>,

</b>"samlsigningcertname":true,

"sendpassword":true,

"samlissuername":true,

"relaystaterule":true,

"signaturealg":true,

"digestmethod":true,
```

```
"audience":true,

"nameidformat":true,

"nameidexpr":true,

"attribute1":true,

"attribute1friendlyname":true,

"attribute1format":true,

"attribute2":true,

"attribute2friendlyname":true,

"attribute2format":true,

"attribute3":true,

"attribute3friendlyname":true,

"attribute3format":true,

"attribute4":true,

"attribute4friendlyname":true,

"attribute4format":true,

"attribute5":true,

"attribute5friendlyname":true,

"attribute5format":true,

"attribute6":true,

"attribute6friendlyname":true,

"attribute6format":true,

"attribute7":true,
```

```
"attribute7friendlyname":true,

"attribute7format":true,

"attribute8":true,

"attribute8friendlyname":true,

"attribute8format":true,

"attribute9":true,

"attribute9friendlyname":true,

"attribute9format":true,

"attribute10":true,

"attribute10friendlyname":true,

"attribute10format":true,

"attribute11":true,

"attribute11friendlyname":true,

"attribute11format":true,

"attribute12":true,

"attribute12friendlyname":true,

"attribute12format":true,

"attribute13":true,

"attribute13friendlyname":true,

"attribute13format":true,

"attribute14":true,

"attribute14friendlyname":true,
```

```
"attribute14format":true,

"attribute15":true,

"attribute15friendlyname":true,

"attribute15format":true,

"attribute16":true,

"attribute16friendlyname":true,

"attribute16format":true,

"encryptassertion":true,

"samlspcertname":true,

"encryptionalgorithm":true,

"skewtime":true,

"signassertion":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/tmsamlssoprofile **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/tmsamlssoprofile? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/tmsamlssoprofile? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of tmsamlssoprofile resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/tmsamlssoprofile? **view=summary**

Use this query-parameter to get the summary output of tmsamlssoprofile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/tmsamlssoprofile? **pagesize=#no;pageno=#no**

Use this query-parameter to get the tmsamlssoprofile resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "tmsamlssoprofile": [ {

"name":<String_value>,

"samlsigningcertname":<String_value>,

"assertionconsumerserviceurl":<String_value>,

"sendpassword":<String_value>,

"samlissuername":<String_value>,
```

```
"relaystaterule":<String_value>,

"signaturealg":<String_value>,

"digestmethod":<String_value>,

"audience":<String_value>,

"nameidformat":<String_value>,

"nameidexpr":<String_value>,

"attribute1":<String_value>,

"attribute2":<String_value>,

"attribute3":<String_value>,

"attribute4":<String_value>,

"attribute5":<String_value>,

"attribute6":<String_value>,

"attribute7":<String_value>,

"attribute8":<String_value>,

"attribute9":<String_value>,

"attribute10":<String_value>,

"attribute11":<String_value>,

"attribute12":<String_value>,

"attribute13":<String_value>,

"attribute14":<String_value>,

"attribute15":<String_value>,

"attribute16":<String_value>,
```

```
"attribute1friendlyname":<String_value>,

"attribute2friendlyname":<String_value>,

"attribute3friendlyname":<String_value>,

"attribute4friendlyname":<String_value>,

"attribute5friendlyname":<String_value>,

"attribute6friendlyname":<String_value>,

"attribute7friendlyname":<String_value>,

"attribute8friendlyname":<String_value>,

"attribute9friendlyname":<String_value>,

"attribute10friendlyname":<String_value>,

"attribute11friendlyname":<String_value>,

"attribute12friendlyname":<String_value>,

"attribute13friendlyname":<String_value>,

"attribute14friendlyname":<String_value>,

"attribute15friendlyname":<String_value>,

"attribute16friendlyname":<String_value>,

"attribute1format":<String_value>,

"attribute2format":<String_value>,

"attribute3format":<String_value>,

"attribute4format":<String_value>,

"attribute5format":<String_value>,

"attribute6format":<String_value>,
```

```
"attribute7format":<String_value>,

"attribute8format":<String_value>,

"attribute9format":<String_value>,

"attribute10format":<String_value>,

"attribute11format":<String_value>,

"attribute12format":<String_value>,

"attribute13format":<String_value>,

"attribute14format":<String_value>,

"attribute15format":<String_value>,

"attribute16format":<String_value>,

"attribute1expr":<String_value>,

"attribute2expr":<String_value>,

"attribute3expr":<String_value>,

"attribute4expr":<String_value>,

"attribute5expr":<String_value>,

"attribute6expr":<String_value>,

"attribute7expr":<String_value>,

"attribute8expr":<String_value>,

"attribute9expr":<String_value>,

"attribute10expr":<String_value>,

"attribute11expr":<String_value>,

"attribute12expr":<String_value>,
```

```
"attribute13expr":<String_value>,

"attribute14expr":<String_value>,

"attribute15expr":<String_value>,

"attribute16expr":<String_value>,

"encryptassertion":<String_value>,

"samlspcertname":<String_value>,

"encryptionalgorithm":<String_value>,

"skewtime":<Integer_value>,

"signassertion":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/tmsamlssoprofile/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/tmsamlssoprofile/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/tmsamlssoprofile/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of tmsamlssoprofile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "tmsamlssoprofile": [ {

"name":<String_value>,

"samlsigningcertname":<String_value>,

"assertionconsumerserviceurl":<String_value>,

"sendpassword":<String_value>,

"samlissuername":<String_value>,

"relaystaterule":<String_value>,

"signaturealg":<String_value>,

"digestmethod":<String_value>,

"audience":<String_value>,

"nameidformat":<String_value>,

"nameidexpr":<String_value>,

"attribute1":<String_value>,

"attribute2":<String_value>,

"attribute3":<String_value>,
```

```
"attribute4":<String_value>,

"attribute5":<String_value>,

"attribute6":<String_value>,

"attribute7":<String_value>,

"attribute8":<String_value>,

"attribute9":<String_value>,

"attribute10":<String_value>,

"attribute11":<String_value>,

"attribute12":<String_value>,

"attribute13":<String_value>,

"attribute14":<String_value>,

"attribute15":<String_value>,

"attribute16":<String_value>,

"attribute1friendlyname":<String_value>,

"attribute2friendlyname":<String_value>,

"attribute3friendlyname":<String_value>,

"attribute4friendlyname":<String_value>,

"attribute5friendlyname":<String_value>,

"attribute6friendlyname":<String_value>,

"attribute7friendlyname":<String_value>,

"attribute8friendlyname":<String_value>,

"attribute9friendlyname":<String_value>,
```

```
"attribute10friendlyname":<String_value>,

"attribute11friendlyname":<String_value>,

"attribute12friendlyname":<String_value>,

"attribute13friendlyname":<String_value>,

"attribute14friendlyname":<String_value>,

"attribute15friendlyname":<String_value>,

"attribute16friendlyname":<String_value>,

"attribute1format":<String_value>,

"attribute2format":<String_value>,

"attribute3format":<String_value>,

"attribute4format":<String_value>,

"attribute5format":<String_value>,

"attribute6format":<String_value>,

"attribute7format":<String_value>,

"attribute8format":<String_value>,

"attribute9format":<String_value>,

"attribute10format":<String_value>,

"attribute11format":<String_value>,

"attribute12format":<String_value>,

"attribute13format":<String_value>,

"attribute14format":<String_value>,

"attribute15format":<String_value>,
```

```
"attribute16format":<String_value>,

"attribute1expr":<String_value>,

"attribute2expr":<String_value>,

"attribute3expr":<String_value>,

"attribute4expr":<String_value>,

"attribute5expr":<String_value>,

"attribute6expr":<String_value>,

"attribute7expr":<String_value>,

"attribute8expr":<String_value>,

"attribute9expr":<String_value>,

"attribute10expr":<String_value>,

"attribute11expr":<String_value>,

"attribute12expr":<String_value>,

"attribute13expr":<String_value>,

"attribute14expr":<String_value>,

"attribute15expr":<String_value>,

"attribute16expr":<String_value>,

"encryptassertion":<String_value>,

"samlspcertname":<String_value>,

"encryptionalgorithm":<String_value>,

"skewtime":<Integer_value>,

"signassertion":<String_value>,
```

```
"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/tmsamlssoprofile? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "tmsamlssoprofile": [ { "__count": "#no"} ] }
```

tmsessionaction

Configuration for TM session action resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the session action. Must begin with an ASCII alphanumeric or

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after a session action is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my action" or 'my action'). Minimum length = 1
sesstimeout	<Integer>	Read-write	Session timeout, in minutes. If there is no traffic during the timeout period, the user is disconnected and must reauthenticate to access intranet resources. Minimum value = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
defaultauthorizationaction	<String>	Read-write	Allow or deny access to content for which there is no specific authorization policy. Possible values = ALLOW, DENY
sso	<String>	Read-write	Use single sign-on (SSO) to log users on to all web applications automatically after they authenticate, or pass users to the web application logon page to authenticate to each application individually. Note that this configuration does not honor the following authentication types for security reason. BASIC, DIGEST, and NTLM (without Negotiate NTLM2 Key or Negotiate Sign Flag). Use TM TrafficAction to configure SSO for these authentication types. Default value: OFF Possible values = ON, OFF
ssocredential	<String>	Read-write	Use the primary or secondary

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			authentication credentials for single sign-on (SSO). Possible values = PRIMARY, SECONDARY
ssodomain	<String>	Read-write	Domain to use for single sign-on (SSO). Minimum length = 1 Maximum length = 32
httponlycookie	<String>	Read-write	Allow only an HTTP session cookie, in which case the cookie cannot be accessed by scripts. Default value: YES Possible values = YES, NO
kcdaccount	<String>	Read-write	Kerberos constrained delegation account name. Minimum length = 1 Maximum length = 32
persistentcookie	<String>	Read-write	Enable or disable persistent SSO cookies for the traffic management (TM) session. A persistent cookie remains on the user device and

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			is sent with each HTTP request. The cookie becomes stale if the session ends. This setting is overwritten if a traffic action sets persistent cookie to OFF. Note: If persistent cookie is enabled, make sure you set the persistent cookie validity. Possible values = ON, OFF
persistentcookievalidity	<Integer>	Read-write	Integer specifying the number of minutes for which the persistent cookie remains valid. Can be set only if the persistent cookie setting is enabled. Minimum value = 1
homepage	<String>	Read-write	Web address of the home page that a user is displayed when authentication vserver is bookmarked and used to login.
builtin	<String[]>	Read-only	Indicates that a variable is a built-in (SYSTEM INTERNAL) type.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL
feature	<String>	Read-only	The feature to be checked while applying this config.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of

creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/tmsessionaction **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"tmsessionaction":{

<b>"name":<String_value>,

</b>"sesstimeout":<Integer_value>,

"defaultauthorizationaction":<String_value>,

"sso":<String_value>,

"ssocredential":<String_value>,

"ssodomain":<String_value>,

"httponlycookie":<String_value>,

"kcdaccount":<String_value>,
```

```
"persistentcookie":<String_value>,

"persistentcookievalidity":<Integer_value>,

"homepage":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/tmsessionaction/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/tmsessionaction **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"tmsessionaction":{

<b>"name":<String_value>,

</b>"sesstimeout":<Integer_value>,
```

```
"defaultauthorizationaction":<String_value>,

"sso":<String_value>,

"ssocredential":<String_value>,

"ssodomain":<String_value>,

"kcdaccount":<String_value>,

"httponlycookie":<String_value>,

"persistentcookie":<String_value>,

"persistentcookievalidity":<Integer_value>,

"homepage":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/tmsessionaction? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"tmsessionaction":{

<b>"name":<String_value>,
```

```
</b>"sesstimeout":true,

"defaultauthorizationaction":true,

"sso":true,

"ssocredential":true,

"ssodomain":true,

"kcdaccount":true,

"httponlycookie":true,

"persistentcookie":true,

"persistentcookievalidity":true,

"homepage":true

}}
```


Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/tmsessionaction **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/tmsessionaction? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/tmsessionaction? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of tmsessionaction resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/tmsessionaction? **view=summary**

Use this query-parameter to get the summary output of tmsessionaction resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/tmsessionaction? **pagesize=#no;pageno=#no**

Use this query-parameter to get the tmsessionaction resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "tmsessionaction": [ {

"name":<String_value>,

"sesstimeout":<Integer_value>,

"defaultauthorizationaction":<String_value>,

"sso":<String_value>,

"ssocredential":<String_value>,

"ssodomain":<String_value>,

"kcdaccount":<String_value>,
```

```
"httponlycookie":<String_value>,

"persistentcookie":<String_value>,

"persistentcookievalidity":<Integer_value>,

"homepage":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/tmsessionaction/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/tmsessionaction/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/tmsessionaction/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of tmsessionaction resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "tmsessionaction": [ {

"name":<String_value>,

"sesstimeout":<Integer_value>,

"defaultauthorizationaction":<String_value>,

"sso":<String_value>,

"ssocredential":<String_value>,

"ssodomain":<String_value>,

"kcdaccount":<String_value>,

"httponlycookie":<String_value>,

"persistentcookie":<String_value>,

"persistentcookievalidity":<Integer_value>,

"homepage":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/tmsessionaction? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "tmsessionaction": [ { "__count": "#no"} ] }
```

tmsessionparameter

Configuration for session parameter resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
sesstimeout	<Integer>	Read-write	Session timeout, in minutes. If there is no traffic during the timeout period, the user is disconnected and must reauthenticate to access the intranet resources.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: 30 Minimum value = 1
defaultauthorizationaction	<String>	Read-write	Allow or deny access to content for which there is no specific authorization policy. Default value: DENY Possible values = ALLOW, DENY
sso	<String>	Read-write	Log users on to all web applications automatically after they authenticate, or pass users to the web application logon page to authenticate for each application. Note that this configuration does not honor the following authentication types for security reason. BASIC, DIGEST, and NTLM (without Negotiate NTLM2 Key or Negotiate Sign Flag). Use TM TrafficAction to configure SSO for these authentication types. Default value: OFF

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ON, OFF
ssocredential	<String>	Read-write	Use primary or secondary authentication credentials for single sign-on. Default value: PRIMARY Possible values = PRIMARY, SECONDARY
ssodomain	<String>	Read-write	Domain to use for single sign-on. Minimum length = 1 Maximum length = 32
kcdaccount	<String>	Read-write	Kerberos constrained delegation account name. Minimum length = 1 Maximum length = 32
httponlycookie	<String>	Read-write	Allow only an HTTP session cookie, in which case the cookie cannot be accessed by scripts. Default value: YES Possible values = YES, NO

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
persistentcookie	<String>	Read-write	Use persistent SSO cookies for the traffic session. A persistent cookie remains on the user device and is sent with each HTTP request. The cookie becomes stale if the session ends. Default value: OFF Possible values = ON, OFF
persistentcookievalidity	<Integer>	Read-write	Integer specifying the number of minutes for which the persistent cookie remains valid. Can be set only if the persistence cookie setting is enabled. Minimum value = 1
homepage	<String>	Read-write	Web address of the home page that a user is displayed when authentication vserver is bookmarked and used to login. Default value: "None"
name	<String>	Read-only	.
tmsessionpolicybindtype	<String>	Read-only	Indicates current bind type (Classic/ Advanced) for TM

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			session policy across all bind entities. Default value: Advanced Policy Possible values = Classic Policy, Advanced Policy
tmsessionpolicycount	<Integer>	Read-only	Count of TM session policies across all bind entities.
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- UPDATE
- UNSET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/tmsessionparameter **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"tmsessionparameter":{

"sesstimeout":<Integer_value>,

"defaultauthorizationaction":<String_value>,

"sso":<String_value>,

"ssocredential":<String_value>,

"ssodomain":<String_value>,

"kcdaccount":<String_value>,

"httponlycookie":<String_value>,

"persistentcookie":<String_value>,

"persistentcookievalidity":<Integer_value>,

"homepage":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/tmsessionparameter? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"tmsessionparameter":{

"sesstimeout":true,

"sso":true,

"ssodomain":true,

"kcdaccount":true,

"persistentcookie":true,

"homepage":true,

"defaultauthorizationaction":true,

"ssocredential":true,

"httponlycookie":true,

"persistentcookievalidity":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/tmsessionparameter **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "tmsessionparameter": [ {

"name":<String_value>,

"sesstimeout":<Integer_value>,

"defaultauthorizationaction":<String_value>,

"sso":<String_value>,

"ssocredential":<String_value>,

"ssodomain":<String_value>,

"kcdaccount":<String_value>,

"httponlycookie":<String_value>,
```

```
"homepage":<String_value>,

"persistentcookie":<String_value>,

"persistentcookievalidity":<Integer_value>,

"tmsessionpolicybindtype":<String_value>,

"tmsessionpolicycount":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

tmsessionpolicy

Configuration for TM session policy resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the session policy. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at sign (@), equal sign (=), and hyphen (-) characters. Cannot be changed after a session policy is created.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my policy" or 'my policy'). Minimum length = 1
rule	<String>	Read-write	Expression, against which traffic is evaluated. Both classic and advance expressions are supported in default partition but only advance expressions in non-default partition. The following requirements apply only to the Citrix ADC CLI: * If the expression includes one or more spaces, enclose the entire expression in double quotation marks.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			* If the expression itself includes double quotation marks, escape the quotations by using the \ character. * Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks.
action	<String>	Read-write	Action to be applied to connections that match this policy. Minimum length = 1
builtin	<String[]>	Read-only	Indicates that a variable is a built-in (SYSTEM INTERNAL) type. Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL
feature	<String>	Read-only	The feature to be checked while applying this config.
expressiontype	<String>	Read-only	Type of policy (Classic/Advanced) .

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = Classic Policy, Advanced Policy
hits	<Integer>	Read-only	Number of hits.
gotopriorityexpression	<String>	Read-only	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/tmsessionpolicy **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"tmsessionpolicy":{

<b>"name":<String_value>,

</b><b>"rule":<String_value>,

</b><b>"action":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/tmsessionpolicy/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/tmsessionpolicy **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"tmsessionpolicy":{

<b>"name":<String_value>,

</b>"rule":<String_value>,

"action":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/tmsessionpolicy? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"tmsessionpolicy":{

<b>"name":<String_value>,

</b>"rule":true,

"action":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/tmsessionpolicy **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/tmsessionpolicy? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/tmsessionpolicy? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of tmsessionpolicy resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/tmsessionpolicy? **view=summary**

Use this query-parameter to get the summary output of tmsessionpolicy resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/tmsessionpolicy? **pagesize=#no;pageno=#no**

Use this query-parameter to get the tmsessionpolicy resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "tmsessionpolicy": [ {

"name":<String_value>,

"rule":<String_value>,

"action":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"expressiontype":<String_value>,

"hits":<Integer_value>,
```

```
"gotopriorityexpression":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/tmsessionpolicy/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/tmsessionpolicy/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/tmsessionpolicy/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of tmsessionpolicy resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "tmsessionpolicy": [ {

"name":<String_value>,

"rule":<String_value>,

"action":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"expressiontype":<String_value>,

"hits":<Integer_value>,

"gotopriorityexpression":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/tmsessionpolicy? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "tmsessionpolicy": [ { "__count": "#no"} ] }
```

tmsessionpolicy_aaagroup_binding

Binding object showing the aaagroup that can be bound to tmsessionpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
boundto	<String>	Read-write	The entity name to which policy is bound.
name	<String>	Read-write	Name of the session policy for which to display detailed information. Minimum length = 1
priority	<Integer>	Read-only	.
activepolicy	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/tmsessionpolicy_aaagroup_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ tmsessionpolicy_aaagroup_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of tmsessionpolicy_aaagroup_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/tmsessionpolicy_aaagroup_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the tmsessionpolicy_aaagroup_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "tmsessionpolicy_aaagroup_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"priority":<Integer_value>,

"activepolicy":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/tmsessionpolicy_aaagroup_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/tmsessionpolicy_aaagroup_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "tmsessionpolicy_aaagroup_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"priority":<Integer_value>,

"activepolicy":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/tmsessionpolicy_aaagroup_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"tmsessionpolicy_aaagroup_binding": [ { "__count": "#no"} ] }
```

tmsessionpolicy_aaauser_binding

Binding object showing the aaauser that can be bound to tmsessionpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
boundto	<String>	Read-write	The entity name to which policy is bound.
name	<String>	Read-write	Name of the session policy for which to display detailed information. Minimum length = 1
activepolicy	<Integer>	Read-only	.
priority	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/tmsessionpolicy_aaauser_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ tmsessionpolicy_aaauser_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of tmsessionpolicy_aaauser_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/tmsessionpolicy_aaauser_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the tmsessionpolicy_aaauser_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "tmsessionpolicy_aaauser_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"activepolicy":<Integer_value>,

"priority":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/tmsessionpolicy_aaauser_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/tmsessionpolicy_aaauser_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "tmsessionpolicy_aaauser_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"activepolicy":<Integer_value>,

"priority":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/tmsessionpolicy_aaauser_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"tmsessionpolicy_aaauser_binding": [ { "__count": "#no"} ] }
```

tmsessionpolicy_authenticationvserver_binding

Binding object showing the authenticationvserver that can be bound to tmsessionpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
boundto	<String>	Read-write	The entity name to which policy is bound.
name	<String>	Read-write	Name of the session policy for which to display detailed information. Minimum length = 1
activepolicy	<Integer>	Read-only	.
priority	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/tmsessionpolicy_authenticationvserver_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/tmsessionpolicy_authenticationvserver_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of tmsessionpolicy_authenticationvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/tmsessionpolicy_authenticationvserver_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the tmsessionpolicy_authenticationvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "tmsessionpolicy_authenticationvserver_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"activepolicy":<Integer_value>,

"priority":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/tmsessionpolicy_authenticationvserver_binding
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/tmsessionpolicy_authenticationvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "tmsessionpolicy_authenticationvserver_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"activepolicy":<Integer_value>,

"priority":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/ tmsessionpolicy_authenticationvserver_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"tmsessionpolicy_authenticationvserver_binding": [ { "__count":
"#no"} ] }
```

tmsessionpolicy_binding

Binding object which returns the resources bound to tmsessionpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the session policy for which to display detailed information. Minimum length = 1
tmsessionpolicy_authenticationvserver_binding	<tmsessionpolicy_authenticationvserver_binding[]>	Read-only	authenticationvserver that can be bound to tmsessionpolicy.
tmsessionpolicy_aaauser_binding	<tmsessionpolicy_aaauser_binding[]>	Read-only	aaauser that can be bound to tmsessionpolicy.
tmsessionpolicy_aaagroup_binding	<tmsessionpolicy_aaagroup_binding[]>	Read-only	aaagroup that can be bound to tmsessionpolicy.
tmsessionpolicy_tmglobal_binding	<tmsessionpolicy_tmglobal_binding[]>	Read-only	tmglobal that can be bound to tmsessionpolicy.

Operations

(click to see Properties)

- GET

- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/tmsessionpolicy_binding/ name_value<String>
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "tmsessionpolicy_binding": [ {

"name":<String_value>,

"tmsessionpolicy_authenticationvserver_binding":<tmsessionpolicy_authentic
ationvserver_binding[]_value>,

"tmsessionpolicy_aaauser_binding":<tmsessionpolicy_aaauser_binding[]_value
>,

"tmsessionpolicy_tmglobal_binding":<tmsessionpolicy_tmglobal_binding[]_val
ue>,

"tmsessionpolicy_aaagroup_binding":<tmsessionpolicy_aaagroup_binding[]_val
ue>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/tmsessionpolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/tmsessionpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "tmsessionpolicy_binding": [ {

"name":<String_value>,

"tmsessionpolicy_authenticationvserver_binding":<tmsessionpolicy_authentic
ationvserver_binding[]_value>,

"tmsessionpolicy_aaauser_binding":<tmsessionpolicy_aaauser_binding[]_value
>,

"tmsessionpolicy_tmglobal_binding":<tmsessionpolicy_tmglobal_binding[]_val
ue>,

"tmsessionpolicy_aaagroup_binding":<tmsessionpolicy_aaagroup_binding[]_val
ue>

}]}
```

tmsessionpolicy_tmglobal_binding

Binding object showing the tmglobal that can be bound to tmsessionpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the session policy for which to display detailed information. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
boundto	<String>	Read-write	The entity name to which policy is bound.
activepolicy	<Integer>	Read-only	.
priority	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/tmsessionpolicy_tmglobal_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ tmsessionpolicy_tmglobal_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of tmsessionpolicy_tmglobal_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/tmsessionpolicy_tmglobal_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the tmsessionpolicy_tmglobal_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "tmsessionpolicy_tmglobal_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"activepolicy":<Integer_value>,
```

```
"priority":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/tmsessionpolicy_tmglobal_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/tmsessionpolicy_tmglobal_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "tmsessionpolicy_tmglobal_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"activepolicy":<Integer_value>,

"priority":<Integer_value>
```

```
}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/tmsessionpolicy_tmglobal_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"tmsessionpolicy_tmglobal_binding": [ { "__count": "#no"} ] }
```

tmtrafficaction

Configuration for TM traffic action resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the traffic action. Must begin with an ASCII alphanumeric or underscore (_) character, and must

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after a traffic action is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my action" or 'my action'). Minimum length = 1
apptimeout	<Integer>	Read-write	Time interval, in minutes, of user inactivity after which the connection is closed. Minimum value = 1 Maximum value = 715827
sso	<String>	Read-write	Use single sign-on for the resource that

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			the user is accessing now. Possible values = ON, OFF
formssoaction	<String>	Read-write	Name of the configured form-based single sign-on profile.
persistentcookie	<String>	Read-write	Use persistent cookies for the traffic session. A persistent cookie remains on the user device and is sent with each HTTP request. The cookie becomes stale if the session ends. Possible values = ON, OFF
initiatelogout	<String>	Read-write	Initiate logout for the traffic management (TM) session if the policy evaluates to true. The session is then terminated after two minutes. Possible values = ON, OFF
kcdaccount	<String>	Read-write	Kerberos constrained delegation account name. Default value: "None"

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum length = 1 Maximum length = 32
samlssoprofile	<String>	Read-write	Profile to be used for doing SAML SSO to remote relying party. Minimum length = 1
forcedtimeout	<String>	Read-write	Setting to start, stop or reset TM session force timer. Possible values = START, STOP, RESET
forcedtimeoutval	<Integer>	Read-write	Time interval, in minutes, for which force timer should be set.
userexpression	<String>	Read-write	expression that will be evaluated to obtain username for SingleSignOn. Maximum length = 256
passwdexpression	<String>	Read-write	expression that will be evaluated to obtain password for SingleSignOn. Maximum length = 256
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/tmtrafficaction **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"tmtrafficaction":{

<b>"name":<String_value>,

</b>"apptimeout":<Integer_value>,

"sso":<String_value>,

"formssoaction":<String_value>,

"persistentcookie":<String_value>,

"initiatelogout":<String_value>,

"kcdaccount":<String_value>,

"samlssoprofile":<String_value>,

"forcedtimeout":<String_value>,

"forcedtimeoutval":<Integer_value>,

"userexpression":<String_value>,

"passwdexpression":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/tmtrafficaction/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/tmtrafficaction **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"tmtrafficaction":{

<b>"name":<String_value>,

</b>"apptimeout":<Integer_value>,

"sso":<String_value>,

"formssoaction":<String_value>,

"persistentcookie":<String_value>,

"initiatelogout":<String_value>,

"kcdaccount":<String_value>,

"samlssoprofile":<String_value>,

"forcedtimeout":<String_value>,
```

```
"forcedtimeoutval":<Integer_value>,

"userexpression":<String_value>,

"passwdexpression":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/tmtrafficaction? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"tmtrafficaction":{

<b>"name":<String_value>,

</b>"persistentcookie":true,

"kcdaccount":true,

"forcedtimeout":true,

"userexpression":true,

"passwdexpression":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/tmtrafficaction **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/tmtrafficaction? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/tmtrafficaction? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of tmtrafficaction resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/tmtrafficaction? **view=summary**

Use this query-parameter to get the summary output of tmtrafficaction resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/tmtrafficaction? **pagesize=#no;pageno=#no**

Use this query-parameter to get the tmtrafficaction resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "tmtrafficaction": [ {

"name":<String_value>,

"apptimeout":<Integer_value>,

"sso":<String_value>,

"formssoaction":<String_value>,

"persistentcookie":<String_value>,

"initiatelogout":<String_value>,

"kcdaccount":<String_value>,

"samlssoprofile":<String_value>,

"forcedtimeout":<String_value>,

"forcedtimeoutval":<Integer_value>,

"userexpression":<String_value>,

"passwdexpression":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/tmtrafficaction/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/tmtrafficaction/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/tmtrafficaction/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of tmtrafficaction resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "tmtrafficaction": [ {

"name":<String_value>,

"apptimeout":<Integer_value>,

"sso":<String_value>,

"formssoaction":<String_value>,

"persistentcookie":<String_value>,

"initiatelogout":<String_value>,

"kcdaccount":<String_value>,

"samlssoprofile":<String_value>,
```

```
"forcedtimeout":<String_value>,

"forcedtimeoutval":<Integer_value>,

"userexpression":<String_value>,

"passwdexpression":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/tmtrafficaction? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "tmtrafficaction": [ { "__count": "#no"} ] }
```

tmtrafficpolicy

Configuration for TM traffic policy resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the traffic policy. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the policy is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my policy" or 'my policy'). Minimum length = 1
rule	<String>	Read-write	Name of the Citrix ADC named expression, or an expression, that the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			policy uses to determine whether to apply certain action on the current traffic.
action	<String>	Read-write	Name of the action to apply to requests or connections that match this policy. Minimum length = 1
hits	<Integer>	Read-only	Number of hits.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/tmtrafficpolicy **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"tmtrafficpolicy":{

<b>"name":<String_value>,

</b><b>"rule":<String_value>,

</b><b>"action":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/tmtrafficpolicy/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/tmtrafficpolicy **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"tmtrafficpolicy":{

<b>"name":<String_value>,

</b>"rule":<String_value>,

"action":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/tmtrafficpolicy? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"tmtrafficpolicy":{

<b>"name":<String_value>,

</b>"rule":true,

"action":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/tmtrafficpolicy **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/tmtrafficpolicy? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/tmtrafficpolicy? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of tmtrafficpolicy resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/tmtrafficpolicy? **view=summary**

Use this query-parameter to get the summary output of tmtrafficpolicy resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/tmtrafficpolicy? **pagesize=#no;pageno=#no**

Use this query-parameter to get the tmtrafficpolicy resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "tmtrafficpolicy": [ {

"name":<String_value>,

"rule":<String_value>,

"action":<String_value>,

"hits":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/tmtrafficpolicy/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/tmtrafficpolicy/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/tmtrafficpolicy/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of tmtrafficpolicy resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "tmtrafficpolicy": [ {

"name":<String_value>,

"rule":<String_value>,

"action":<String_value>,

"hits":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/tmtrafficpolicy? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "tmtrafficpolicy": [ { "__count": "#no"} ] }
```

tmtrafficpolicy_binding

Binding object which returns the resources bound to tmtrafficpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the traffic policy for which to display detailed information. Minimum length = 1
tmtrafficpolicy_tmglobal_binding	<tmtrafficpolicy_tmglobal_binding[]>	Read-only	tmglobal that can be bound to tmtrafficpolicy.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
tmtrafficpolicy_csvserver_binding	<tmtrafficpolicy_csvserver_binding[]>	Read-only	csvserver that can be bound to tmtrafficpolicy.
tmtrafficpolicy_lbvserver_binding	<tmtrafficpolicy_lbvserver_binding[]>	Read-only	lbvserver that can be bound to tmtrafficpolicy.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/tmtrafficpolicy_binding/ name_value<String>
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "tmtrafficpolicy_binding": [ {

"name":<String_value>,

"tmtrafficpolicy_csvserver_binding":<tmtrafficpolicy_csvserver_binding[]_v
alue>,

"tmtrafficpolicy_tmglobal_binding":<tmtrafficpolicy_tmglobal_binding[]_val
ue>,

"tmtrafficpolicy_lbvserver_binding":<tmtrafficpolicy_lbvserver_binding[]_v
alue>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/tmtrafficpolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/tmtrafficpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "tmtrafficpolicy_binding": [ {

"name":<String_value>,

"tmtrafficpolicy_csvserver_binding":<tmtrafficpolicy_csvserver_binding[]_value>,

"tmtrafficpolicy_tmglobal_binding":<tmtrafficpolicy_tmglobal_binding[]_value>,

"tmtrafficpolicy_lbvserver_binding":<tmtrafficpolicy_lbvserver_binding[]_value>

}]}
```

tmtrafficpolicy_csvserver_binding

Binding object showing the csvserver that can be bound to tmtrafficpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
boundto	<String>	Read-write	The entity name to which policy is bound.
name	<String>	Read-write	Name of the traffic policy for which to display detailed information. Minimum length = 1
activepolicy	<Integer>	Read-only	.
priority	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/tmtrafficpolicy_csvserver_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ tmtrafficpolicy_csvserver_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of tmtrafficpolicy_csvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/tmtrafficpolicy_csvserver_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the tmtrafficpolicy_csvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "tmtrafficpolicy_csvserver_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"activepolicy":<Integer_value>,

"priority":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/tmtrafficpolicy_csvserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/tmtrafficpolicy_csvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "tmtrafficpolicy_csvserver_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"activepolicy":<Integer_value>,

"priority":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/tmtrafficpolicy_csvserver_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"tmtrafficpolicy_csvserver_binding": [ { "__count": "#no"} ] }
```

tmtrafficpolicy_lbvserver_binding

Binding object showing the lbvserver that can be bound to tmtrafficpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the traffic policy for which to display detailed information. Minimum length = 1
boundto	<String>	Read-write	The entity name to which policy is bound.
priority	<Integer>	Read-only	.
activepolicy	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/tmtrafficpolicy_lbvserver_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ tmtrafficpolicy_lbvserver_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of tmtrafficpolicy_lbvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/tmtrafficpolicy_lbvserver_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the tmtrafficpolicy_lbvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "tmtrafficpolicy_lbvserver_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"priority":<Integer_value>,

"activepolicy":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/tmtrafficpolicy_lbvserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/tmtrafficpolicy_lbvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "tmtrafficpolicy_lbvserver_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"priority":<Integer_value>,

"activepolicy":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/tmtrafficpolicy_lbvserver_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"tmtrafficpolicy_lbvserver_binding": [ { "__count": "#no"} ] }
```

tmtrafficpolicy_tmglobal_binding

Binding object showing the tmglobal that can be bound to tmtrafficpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the traffic policy for which to display detailed information. Minimum length = 1
boundto	<String>	Read-write	The entity name to which policy is bound.
priority	<Integer>	Read-only	.
activepolicy	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/tmtrafficpolicy_tmglobal_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ tmtrafficpolicy_tmglobal_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of tmtrafficpolicy_tmglobal_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/tmtrafficpolicy_tmglobal_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the tmtrafficpolicy_tmglobal_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "tmtrafficpolicy_tmglobal_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"priority":<Integer_value>,

"activepolicy":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/tmtrafficpolicy_tmglobal_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/tmtrafficpolicy_tmglobal_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "tmtrafficpolicy_tmglobal_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"priority":<Integer_value>,

"activepolicy":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/tmtrafficpolicy_tmglobal_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"tmtrafficpolicy_tmglobal_binding": [ { "__count": "#no"} ] }
```

transform

Transform

URL Transformation configuration.

NAME	DESCRIPTION
transformaction	Configuration for transform action
transformglobal_binding	Binding object showing the resources that can be bound to transformglobal
transformglobal_transformpolicy_binding	Binding object showing the transformpolicy that can be bound to transformglobal
transformpolicy	Configuration for URL Transformation policy
transformpolicy_binding	Binding object showing the resources that can be bound to transformpolicy
transformpolicy_csvserver_binding	Binding object showing the csvserver that can be bound to transformpolicy
transformpolicy_lbvserver_binding	Binding object showing the lbvserver that can be bound to transformpolicy
transformpolicy_transformglobal_binding	Binding object showing the transformglobal that can be bound to transformpolicy
transformpolicy_transformpolicylabel_binding	Binding object showing the transformpolicylabel that can be bound to transformpolicy
transformpolicylabel	Configuration for transform policy label
transformpolicylabel_binding	Binding object showing the resources that can be bound to transformpolicylabel

NAME	DESCRIPTION
transformpolicylabel_policybinding_binding	Binding object showing the policybinding that can be bound to transformpolicylabel
transformpolicylabel_transformpolicy_binding	Binding object showing the transformpolicy that can be bound to transformpolicylabel
transformprofile	Configuration for URL Transformation profile
transformprofile_binding	Binding object showing the resources that can be bound to transformprofile
transformprofile_transformaction_binding	Binding object showing the transformaction that can be bound to transformprofile

transformaction

Configuration for transform action resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the URL transformation action. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@),

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			equals (=), colon (:), and underscore characters. Cannot be changed after the URL Transformation action is added. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, my transform action or my transform action). Minimum length = 1
profilename	<String>	Read-write	Name of the URL Transformation profile with which to associate this action. Minimum length = 1
priority	<Integer>	Read-write	Positive integer specifying the priority of the action within the profile. A lower number specifies a higher priority. Must be unique within the list of actions bound

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			to the profile. Policies are evaluated in the order of their priority numbers, and the first policy that matches is applied. Minimum value = 1 Maximum value = 2147483647
state	<String>	Read-write	Enable or disable this action. Default value: ENABLED Possible values = ENABLED, DISABLED
requrlfrom	<String>	Read-write	PCRE-format regular expression that describes the request URL pattern to be transformed. Minimum length = 1
requrlinto	<String>	Read-write	PCRE-format regular expression that describes the transformation to be performed on URLs that match the reqUrlFrom pattern. Minimum length = 1
resurlfrom	<String>	Read-write	PCRE-format regular expression that describes the response URL

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			pattern to be transformed. Minimum length = 1
resurlinto	<String>	Read-write	PCRE-format regular expression that describes the transformation to be performed on URLs that match the resUrlFrom pattern. Minimum length = 1
cookiedomainfrom	<String>	Read-write	Pattern that matches the domain to be transformed in Set-Cookie headers. Minimum length = 1
cookiedomaininto	<String>	Read-write	PCRE-format regular expression that describes the transformation to be performed on cookie domains that match the cookieDomainFrom pattern. NOTE: The cookie domain to be transformed is extracted from the request. Minimum length = 1
comment	<String>	Read-write	Any comments to preserve information about this URL

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Transformation action.
continuematching	<String>	Read-only	Continue transforming using the next rule in the list. Possible values = ON, OFF
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of

creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/transformaction **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"transformaction":{

<b>"name":<String_value>,

</b><b>"profilename":<String_value>,

</b><b>"priority":<Integer_value>,

</b>"state":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/transformaction/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/transformaction **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"transformaction":{

<b>"name":<String_value>,

</b>"priority":<Integer_value>,

"requrlfrom":<String_value>,

"requrlinto":<String_value>,

"resurlfrom":<String_value>,

"resurlinto":<String_value>,

"cookiedomainfrom":<String_value>,

"cookiedomaininto":<String_value>,

"state":<String_value>,
```

```
"comment":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/transformaction? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"transformaction":{

<b>"name":<String_value>,

</b>"requrlfrom":true,

"requrlinto":true,

"resurlfrom":true,

"resurlinto":true,

"cookiedomainfrom":true,

"cookiedomaininto":true,

"state":true,

"comment":true
```

```
}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/transformaction **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/transformaction? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/transformaction? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of transformaction resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/transformaction? **view=summary**

Use this query-parameter to get the summary output of transformaction resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/transformaction? **pagesize=#no;pageno=#no**

Use this query-parameter to get the transformaction resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "transformaction": [ {

"name":<String_value>,

"profilename":<String_value>,

"priority":<Integer_value>,

"requrlfrom":<String_value>,

"requrlinto":<String_value>,

"resurlfrom":<String_value>,

"resurlinto":<String_value>,

"cookiedomainfrom":<String_value>,

"cookiedomaininto":<String_value>,

"continuematching":<String_value>,

"state":<String_value>,

"comment":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/transformaction/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/transformaction/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/transformaction/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of transformaction resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "transformaction": [ {

"name":<String_value>,

"profilename":<String_value>,

"priority":<Integer_value>,

"requrlfrom":<String_value>,
```

```
"requrlinto":<String_value>,

"resurlfrom":<String_value>,

"resurlinto":<String_value>,

"cookiedomainfrom":<String_value>,

"cookiedomaininto":<String_value>,

"continuematching":<String_value>,

"state":<String_value>,

"comment":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/transformaction? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "transformaction": [ { "__count": "#no"} ] }
```

transformglobal_binding

Binding object which returns the resources bound to transformglobal.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
transformglobal_transformpolicy_binding	<transformglobal_transformpolicy_binding []>	Read-write	transformpolicy that can be bound to transformglobal.

Operations

(click to see Properties)

- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/transformglobal_binding

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "transformglobal_binding": [ {

"transformglobal_transformpolicy_binding":<transformglobal_transformpolicy
_binding[]_value>

}]}
```

transformglobal_transformpolicy_binding

Binding object showing the transformpolicy that can be bound to transformglobal.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
labelname	<String>	Read-write	Name of the policy label to invoke if the current policy evaluates to TRUE, the invoke parameter is set, and the label type is Policy Label.
priority	<Integer>	Read-write	Specifies the priority of the policy.
labeltype	<String>	Read-write	Type of invocation. Available settings function as follows: * reqvserver - Send the request to the specified request virtual server. * resvserver - Send the response to the specified response virtual server. * policylabel - Invoke the specified policy label. Possible values = reqvserver, resvserver, policylabel
invoke	<Boolean>	Read-write	If the current policy evaluates to TRUE, terminate evaluation of policies bound to the current policy label, and then forwards the request

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			or response to the specified virtual server or evaluates the specified policy label.
gotopriorityexpression	<String>	Read-write	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
globalbindtype	<String>	Read-write	. Default value: SYSTEM_GLOBAL Possible values = SYSTEM_GLOBAL, VPN_GLOBAL, RNAT_GLOBAL, APPFW_GLOBAL, TM_GLOBAL
policyname	<String>	Read-write	Name of the transform policy.
type	<String>	Read-write	Specifies the bind point to which to bind the policy. Available settings function as follows: * REQ_OVERRIDE. Request override. Binds the policy to the priority request queue. * REQ_DEFAULT. Binds the policy to the default request

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			queue. * HTTPQUIC_REQ_OVERRIDE - Binds the policy to the HTTP_QUIC override request queue. * HTTPQUIC_REQ_DEFAULT - Binds the policy to the HTTP_QUIC default request queue. Possible values = REQ_OVERRIDE, REQ_DEFAULT, HTTPQUIC_REQ_OVERRIDE, HTTPQUIC_REQ_DEFAULT
numpol	<Integer>	Read-only	The number of policies bound to the bindpoint.
flowtype	<Integer>	Read-only	flowtype of the bound transform policy.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/transformglobal_transformpolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"transformglobal_transformpolicy_binding":{

<b>"policyname":<String_value>,
```

```
</b><b>"priority":<Integer_value>,

</b>"gotoprioritiyexpression":<String_value>,

"type":<String_value>,

"invoke":<Boolean_value>,

"labeltype":<String_value>,

"labelname":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/transformglobal_transformpolicy_binding **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/transformglobal_transformpolicy_binding? **args= policyname:<String_value>, type: <String_value> ,priority: <Integer_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/transformglobal_transformpolicy_binding **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/transformglobal_transformpolicy_binding? **args=type: <String_value>**

Use this query-parameter to get transformglobal_transformpolicy_binding resources based on additional properties.

filter http:// <netscaler-ip-address> /nitro/v1/config/transformglobal_transformpolicy_binding? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of transformglobal_transformpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ transformglobal_transformpolicy_binding? **pagesize=#no;pageno=#no**

Use this query-parameter to get the transformglobal_transformpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "transformglobal_transformpolicy_binding": [ {

"labelname":<String_value>,

"priority":<Integer_value>,

"labeltype":<String_value>,

"invoke":<Boolean_value>,

"gotopriorityexpression":<String_value>,
```

```
"globalbindtype":<String_value>,

"policyname":<String_value>,

"type":<String_value>,

"numpol":<Integer_value>,

"flowtype":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/transformglobal_transformpolicy_binding?**count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "transformglobal_transformpolicy_binding": [ { "__count": "#no"} ] }
```

transformpolicy

Configuration for URL Transformation policy resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the URL Transformation policy. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Can be changed after the URL Transformation policy is added. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, my transform policy or my transform policy).

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum length = 1
rule	<String>	Read-write	Expression, or name of a named expression, against which to evaluate traffic. The following requirements apply only to the Citrix ADC CLI: * If the expression includes blank spaces, the entire expression must be enclosed in double quotation marks. * If the expression itself includes double quotation marks, you must escape the quotations by using the \ character. * Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks.
profilename	<String>	Read-write	Name of the URL Transformation

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			profile to use to transform requests and responses that match the policy. Minimum length = 1
comment	<String>	Read-write	Any comments to preserve information about this URL Transformation policy.
logaction	<String>	Read-write	Log server to use to log connections that match this policy.
newname	<String>	Read-write	New name for the policy. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			my transform policy or my transform policy). Minimum length = 1
hits	<Integer>	Read-only	Number of hits.
isdefault	<Boolean>	Read-only	A value of true is returned if it is a default transform policy.
builtin	<String[]>	Read-only	Flag to determine if Transform policy is built-in or not. Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL
feature	<String>	Read-only	The feature to be checked while applying this config.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)

- GET
- COUNT
- RENAME

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/transformpolicy **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"transformpolicy":{

<b>"name":<String_value>,

</b><b>"rule":<String_value>,

</b><b>"profilename":<String_value>,

</b>"comment":<String_value>,

"logaction":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/transformpolicy/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/transformpolicy **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"transformpolicy":{

<b>"name":<String_value>,

</b>"rule":<String_value>,

"profilename":<String_value>,

"comment":<String_value>,

"logaction":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/transformpolicy? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"transformpolicy":{

<b>"name":<String_value>,

</b>"comment":true,

"logaction":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

RENAME

URL: http:// <netscaler-ip-address> /nitro/v1/config/transformpolicy? **action=rename HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"transformpolicy":{

<b>"name":<String_value>,

</b><b>"newname":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/transformpolicy **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/transformpolicy? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/transformpolicy? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of transformpolicy resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/transformpolicy? **view=summary**

Use this query-parameter to get the summary output of transformpolicy resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/transformpolicy? **pagesize=#no;pageno=#no**

Use this query-parameter to get the transformpolicy resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "transformpolicy": [ {

"name":<String_value>,

"rule":<String_value>,

"profilename":<String_value>,

"hits":<Integer_value>,

"comment":<String_value>,
```

```
"logaction":<String_value>,

"isdefault":<Boolean_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/transformpolicy/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/transformpolicy/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/transformpolicy/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of transformpolicy resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "transformpolicy": [ {

"name":<String_value>,

"rule":<String_value>,

"profilename":<String_value>,

"hits":<Integer_value>,

"comment":<String_value>,

"logaction":<String_value>,

"isdefault":<Boolean_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/transformpolicy? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "transformpolicy": [ { "__count": "#no"} ] }
```

transformpolicy_binding

Binding object which returns the resources bound to transformpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the URL Transformation policy. Minimum length = 1
transformpolicy_lbvserver_binding	<transformpolicy_lbvserver_binding[]>	Read-only	lbvserver that can be bound to transformpolicy.
transformpolicy_transformpolicylabel_binding	<transformpolicy_transformpolicylabel_binding[]>	Read-only	transformpolicylabel that can be bound to transformpolicy.
transformpolicy_csvserver_binding	<transformpolicy_csvserver_binding[]>	Read-only	csvserver that can be bound to transformpolicy.
transformpolicy_transformglobal_binding	<transformpolicy_transformglobal_binding[]>	Read-only	transformglobal that can be bound to transformpolicy.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/transformpolicy_binding/ name_value<String>
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "transformpolicy_binding": [ {

"name":<String_value>,

"transformpolicy_transformpolicylabel_binding":<transformpolicy_transformp
olicylabel_binding[]_value>,

"transformpolicy_lbvserver_binding":<transformpolicy_lbvserver_binding[]_v
alue>,

"transformpolicy_csvserver_binding":<transformpolicy_csvserver_binding[]_v
alue>,

"transformpolicy_transformglobal_binding":<transformpolicy_transformglobal
_binding[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/transformpolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/transformpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "transformpolicy_binding": [ {

"name":<String_value>,

"transformpolicy_transformpolicylabel_binding":<transformpolicy_transformpolicylabel_binding[]_value>,

"transformpolicy_lbvserver_binding":<transformpolicy_lbvserver_binding[]_value>,

"transformpolicy_csvserver_binding":<transformpolicy_csvserver_binding[]_value>,

"transformpolicy_transformglobal_binding":<transformpolicy_transformglobal_binding[]_value>

}]}
```

transformpolicy_csvserver_binding

Binding object showing the csvserver that can be bound to transformpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
boundto	<String>	Read-write	Location where policy is bound.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the URL Transformation policy. Minimum length = 1
labeltype	<String>	Read-only	Type of policy label invocation. Possible values = reqvserver, policylabel
priority	<Integer>	Read-only	Specifies the priority of the policy.
activepolicy	<Integer>	Read-only	Indicates whether policy is bound or not.
labelname	<String>	Read-only	Name of the label to invoke if the current policy rule evaluates to TRUE.
gotopriorityexpression	<String>	Read-only	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/transformpolicy_csvserver_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ transformpolicy_csvserver_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of transformpolicy_csvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/transformpolicy_csvserver_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the transformpolicy_csvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "transformpolicy_csvserver_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"activepolicy":<Integer_value>,

"labelname":<String_value>,

"gotopriorityexpression":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/transformpolicy_csvserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/transformpolicy_csvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "transformpolicy_csvserver_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"activepolicy":<Integer_value>,

"labelname":<String_value>,

"gotopriorityexpression":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/transformpolicy_csvserver_binding/name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"transformpolicy_csvserver_binding": [ { "__count": "#no"} ] }
```

transformpolicy_lbvserver_binding

Binding object showing the lbvserver that can be bound to transformpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
boundto	<String>	Read-write	Location where policy is bound.
name	<String>	Read-write	Name of the URL Transformation policy. Minimum length = 1
gotopriorityexpression	<String>	Read-only	Expression specifying the priority of the next policy which will get evaluated if the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			current policy rule evaluates to TRUE.
labelname	<String>	Read-only	Name of the label to invoke if the current policy rule evaluates to TRUE.
activepolicy	<Integer>	Read-only	Indicates whether policy is bound or not.
priority	<Integer>	Read-only	Specifies the priority of the policy.
labeltype	<String>	Read-only	Type of policy label invocation. Possible values = reqvserver, policylabel
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/transformpolicy_lbvserver_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ transformpolicy_lbvserver_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of transformpolicy_lbvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/transformpolicy_lbvserver_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the transformpolicy_lbvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "transformpolicy_lbvserver_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"gotopriorityexpression":<String_value>,

"labelname":<String_value>,

"activepolicy":<Integer_value>,

"priority":<Integer_value>,

"labeltype":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/transformpolicy_lbvserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/transformpolicy_lbvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "transformpolicy_lbvserver_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"gotopriorityexpression":<String_value>,

"labelname":<String_value>,

"activepolicy":<Integer_value>,

"priority":<Integer_value>,

"labeltype":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/transformpolicy_lbvserver_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"transformpolicy_lbvserver_binding": [ { "__count": "#no"} ] }
```

transformpolicy_transformglobal_binding

Binding object showing the transformglobal that can be bound to transformpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
boundto	<String>	Read-write	Location where policy is bound.
name	<String>	Read-write	Name of the URL Transformation policy. Minimum length = 1
labeltype	<String>	Read-only	Type of policy label invocation. Possible values = reqvserver, policylabel
priority	<Integer>	Read-only	Specifies the priority of the policy.
activepolicy	<Integer>	Read-only	Indicates whether policy is bound or not.
labelname	<String>	Read-only	Name of the label to invoke if the current

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			policy rule evaluates to TRUE.
gotopriorityexpression	<String>	Read-only	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/transformpolicy_transformglobal_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ transformpolicy_transformglobal_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of transformpolicy_transformglobal_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/transformpolicy_transformglobal_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the transformpolicy_transformglobal_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "transformpolicy_transformglobal_binding": [ {

"boundto":<String_value>,
```

```
"name":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"activepolicy":<Integer_value>,

"labelname":<String_value>,

"gotopriorityexpression":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/transformpolicy_transformglobal_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/transformpolicy_transformglobal_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "transformpolicy_transformglobal_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"activepolicy":<Integer_value>,

"labelname":<String_value>,

"gotopriorityexpression":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/transformpolicy_transformglobal_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"transformpolicy_transformglobal_binding": [ { "__count": "#no"} ] }
```

transformpolicy_transformpolicylabel_binding

Binding object showing the transformpolicylabel that can be bound to transformpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the URL Transformation policy. Minimum length = 1
boundto	<String>	Read-write	Location where policy is bound.
gotopriorityexpression	<String>	Read-only	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
labelname	<String>	Read-only	Name of the label to invoke if the current policy rule evaluates to TRUE.
activepolicy	<Integer>	Read-only	Indicates whether policy is bound or not.
priority	<Integer>	Read-only	Specifies the priority of the policy.
labeltype	<String>	Read-only	Type of policy label invocation. Possible values = reqvserver, policylabel

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/transformpolicy_transformpolicylabel_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ transformpolicy_transformpolicylabel_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of transformpolicy_transformpolicylabel_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ transformpolicy_transformpolicylabel_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the transformpolicy_transformpolicylabel_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "transformpolicy_transformpolicylabel_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"gotopriorityexpression":<String_value>,

"labelname":<String_value>,
```

```
"activepolicy":<Integer_value>,

"priority":<Integer_value>,

"labeltype":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/transformpolicy_transformpolicylabel_binding
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/transformpolicy_transformpolicylabel_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "transformpolicy_transformpolicylabel_binding": [ {

"name":<String_value>,

"boundto":<String_value>,
```

```
"gotopriorityexpression":<String_value>,

"labelname":<String_value>,

"activepolicy":<Integer_value>,

"priority":<Integer_value>,

"labeltype":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/transformpolicy_transformpolicylabel_binding/name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"transformpolicy_transformpolicylabel_binding": [ { "__count": "#no"} ] }
```

transformpolicylabel

Configuration for transform policy label resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
labelname	<String>	Read-write	Name for the policy label. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Can be changed after the URL Transformation policy label is added. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, my transform policylabel or my transform policylabel).
policylabeltype	<String>	Read-write	Types of transformations allowed by the policies bound to the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			label. For URL transformation, always http_req (HTTP Request). Possible values = http_req, httpquic_req
newname	<String>	Read-write	New name for the policy label. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, my transform policylabel or my

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			transform policylabel). Minimum length = 1
numpol	<Integer>	Read-only	Number of polices bound to label.
hits	<Integer>	Read-only	Number of times policy label was invoked.
priority	<Integer>	Read-only	Specifies the priority of the policy.
gotopriorityexpression	<String>	Read-only	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
labeltype	<String>	Read-only	Type of invocation. Available settings function as follows: * reqvserver - Forward the request to the specified request virtual server. * policylabel - Invoke the specified policy label. Possible values = reqvserver, policylabel

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
invoke_labelname	<String>	Read-only	Name of the policy label.
description	<String>	Read-only	Description of the policylabel.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET (ALL)
- GET
- COUNT
- RENAME

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/transformpolicylabel **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"transformpolicylabel":{

<b>"labelname":<String_value>,

</b><b>"policylabeltype":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/transformpolicylabel/ labelname_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

RENAME

URL: http:// <netscaler-ip-address> /nitro/v1/config/transformpolicylabel? **action=rename HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"transformpolicylabel":{

<b>"labelname":<String_value>,

</b><b>"newname":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/transformpolicylabel **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/transformpolicylabel? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/transformpolicylabel? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of transformpolicylabel resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/transformpolicylabel? **view=summary**

Use this query-parameter to get the summary output of transformpolicylabel resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/transformpolicylabel? **pagesize=#no;pageno=#no**

Use this query-parameter to get the transformpolicylabel resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "transformpolicylabel": [ {

"labelname":<String_value>,

"policylabeltype":<String_value>,

"numpol":<Integer_value>,

"hits":<Integer_value>,

"priority":<Integer_value>,

"gotopriorityexpression":<String_value>,

"labeltype":<String_value>,
```

```
"invoke_labelname":<String_value>,

"description":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/transformpolicylabel/ labelname_value<String>
Query-parameters: attrs http:// <netscaler-ip-address> /nitro/v1/config/transformpolicylabel/ labelname_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/transformpolicylabel/ labelname_value<String> ? **view=summary**

Use this query-parameter to get the summary output of transformpolicylabel resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "transformpolicylabel": [ {

"labelname":<String_value>,

"policylabeltype":<String_value>,

"numpol":<Integer_value>,

"hits":<Integer_value>,

"priority":<Integer_value>,

"gotopriorityexpression":<String_value>,

"labeltype":<String_value>,

"invoke_labelname":<String_value>,

"description":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/transformpolicylabel? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "transformpolicylabel": [ { "__count": "#no"} ] }
```

transformpolicylabel_binding

Binding object which returns the resources bound to transformpolicylabel.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
labelname	<String>	Read-write	Name for the policy label. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Can be changed after the URL Transformation policy label is added. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			my transform policylabel or my transform policylabel).
transformpolicylabel_transformpolicy_binding	<transformpolicylabel_transformpolicy_binding[]>	Read-only	transformpolicy that can be bound to transformpolicylabel.
transformpolicylabel_policybinding_binding	<transformpolicylabel_policybinding_binding[]>	Read-only	policybinding that can be bound to transformpolicylabel.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/transformpolicylabel_binding/ labelname_value<String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "transformpolicylabel_binding": [ {

"labelname":<String_value>,

"transformpolicylabel_transformpolicy_binding":<transformpolicylabel_trans
formpolicy_binding[]_value>,

"transformpolicylabel_policybinding_binding":<transformpolicylabel_policyb
inding_binding[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/transformpolicylabel_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/transformpolicylabel_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "transformpolicylabel_binding": [ {

"labelname":<String_value>,

"transformpolicylabel_transformpolicy_binding":<transformpolicylabel_transformpolicy_binding[]_value>,

"transformpolicylabel_policybinding_binding":<transformpolicylabel_policybinding_binding[]_value>

}]}
```

transformpolicylabel_policybinding_binding

Binding object showing the policybinding that can be bound to transformpolicylabel.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
policyname	<String>	Read-write	Name of the URL Transformation policy to bind to the policy label.
invoke	<Boolean>	Read-write	If the current policy evaluates to TRUE, terminate evaluation of policies bound to the current policy label, and then forward the request to the specified virtual server or evaluate the specified policy label.
gotopriorityexpression	<String>	Read-write	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
invoke_labelname	<String>	Read-write	Name of the policy label.
priority	<Integer>	Read-write	Specifies the priority of the policy.
labeltype	<String>	Read-write	Type of invocation. Available settings function as follows: * reqvserver - Forward the request to the specified request virtual server. * policylabel - Invoke the specified policy label.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = reqvserver, policylabel
labelname	<String>	Read-write	Name of the URL Transformation policy label to which to bind the policy.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/transformpolicylabel_policybinding_binding/ labelname_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ transformpolicylabel_policybinding_binding/ labelname_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of transformpolicylabel_policybinding_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ transformpolicylabel_policybinding_binding/ labelname_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the transformpolicylabel_policybinding_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "transformpolicylabel_policybinding_binding": [ {

"policyname":<String_value>,
```

```
"invoke":<Boolean_value>,

"gotopriorityexpression":<String_value>,

"invoke_labelname":<String_value>,

"priority":<Integer_value>,

"labeltype":<String_value>,

"labelname":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/transformpolicylabel_policybinding_binding
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/transformpolicylabel_policybinding_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "transformpolicylabel_policybinding_binding": [ {

"policyname":<String_value>,

"invoke":<Boolean_value>,

"gotopriorityexpression":<String_value>,

"invoke_labelname":<String_value>,

"priority":<Integer_value>,

"labeltype":<String_value>,

"labelname":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/transformpolicylabel_policybinding_binding/ labelname_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"transformpolicylabel_policybinding_binding": [ { "__count": "#no"} ] }
```

transformpolicylabel_transformpolicy_binding

Binding object showing the transformpolicy that can be bound to transformpolicylabel.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
gotopriorityexpression	<String>	Read-write	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
invoke	<Boolean>	Read-write	If the current policy evaluates to TRUE, terminate evaluation of policies bound to the current policy label, and then forward the request to the specified virtual server or evaluate the specified policy label.
policyname	<String>	Read-write	Name of the URL Transformation policy to bind to the policy label.
invoke_labelname	<String>	Read-write	Name of the policy label.
labelname	<String>	Read-write	Name of the URL Transformation policy label to which to bind the policy.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
labeltype	<String>	Read-write	Type of invocation. Available settings function as follows: * reqvserver - Forward the request to the specified request virtual server. * policylabel - Invoke the specified policy label. Possible values = reqvserver, policylabel
priority	<Integer>	Read-write	Specifies the priority of the policy.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/transformpolicylabel_transformpolicy_binding
HTTP Method: PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"transformpolicylabel_transformpolicy_binding":{

<b>"labelname":<String_value>,

</b><b>"policyname":<String_value>,

</b><b>"priority":<Integer_value>,

</b>"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>,
```

```
"labeltype":<String_value>,

"invoke_labelname":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/transformpolicylabel_transformpolicy_binding/ labelname_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ transformpolicylabel_transformpolicy_binding/ labelname_value<String> ? **args= policyname:<String_value>, priority: <Integer_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/transformpolicylabel_transformpolicy_binding/ labelname_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ transformpolicylabel_transformpolicy_binding/ labelname_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of transformpolicylabel_transformpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ transformpolicylabel_transformpolicy_binding/ labelname_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the transformpolicylabel_transformpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "transformpolicylabel_transformpolicy_binding": [ {

"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>,

"policyname":<String_value>,

"invoke_labelname":<String_value>,

"labelname":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/transformpolicylabel_transformpolicy_binding
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/transformpolicylabel_transformpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "transformpolicylabel_transformpolicy_binding": [ {

"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>,

"policyname":<String_value>,

"invoke_labelname":<String_value>,

"labelname":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>
```

```
}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/transformpolicylabel_transformpolicy_binding/labelname_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"transformpolicylabel_transformpolicy_binding": [ { "__count": "#no"} ] }
```

transformprofile

Configuration for URL Transformation profile resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the URL transformation profile. Must begin with a letter, number, or the underscore character (_), and

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after the URL transformation profile is added. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, my transform profile or my transform profile). Minimum length = 1
type	<String>	Read-write	Type of transformation. Always URL for URL Transformation profiles. Possible values = URL
onlytransformabsurlinbody	<String>	Read-write	In the HTTP body, transform only absolute URLs.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Relative URLs are ignored. Possible values = ON, OFF
comment	<String>	Read-write	Any comments to preserve information about this URL Transformation profile.
regexforfindingurlinjavascript	<String>	Read-only	Patclass having regexes to find the URLs in JavaScript.
regexforfindingurlincss	<String>	Read-only	Patclass having regexes to find the URLs in CSS.
regexforfindingurlinxcomponent	<String>	Read-only	Patclass having regexes to find the URLs in X-Component.
regexforfindingurlinxml	<String>	Read-only	Patclass having regexes to find the URLs in XML.
additionalreqheaderslist	<String>	Read-only	Patclass having a list of additional request header names that should transformed.
additionalrespheaderslist	<String>	Read-only	Patclass having a list of additional response header names that should transformed.
_nextgenapiresource	<String>	Read-only	.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/transformprofile **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"transformprofile":{

<b>"name":<String_value>,

</b>"type":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/transformprofile/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/transformprofile **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"transformprofile":{

<b>"name":<String_value>,

</b>"type":<String_value>,

"onlytransformabsurlinbody":<String_value>,

"comment":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/transformprofile? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"transformprofile":{

<b>"name":<String_value>,

</b>"type":true,

"onlytransformabsurlinbody":true,
```

```
"comment":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/transformprofile **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/transformprofile? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/transformprofile? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of transformprofile resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/transformprofile? **view=summary**

Use this query-parameter to get the summary output of transformprofile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/transformprofile? **pagesize=#no;pageno=#no**

Use this query-parameter to get the transformprofile resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "transformprofile": [ {

"name":<String_value>,

"type":<String_value>,

"regexforfindingurlinjavascript":<String_value>,

"regexforfindingurlincss":<String_value>,

"regexforfindingurlinxcomponent":<String_value>,

"regexforfindingurlinxml":<String_value>,

"additionalreqheaderslist":<String_value>,

"additionalrespheaderslist":<String_value>,

"onlytransformabsurlinbody":<String_value>,

"comment":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/transformprofile/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/transformprofile/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/transformprofile/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of transformprofile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "transformprofile": [ {

"name":<String_value>,

"type":<String_value>,

"regexforfindingurlinjavascript":<String_value>,

"regexforfindingurlincss":<String_value>,

"regexforfindingurlinxcomponent":<String_value>,

"regexforfindingurlinxml":<String_value>,

"additionalreqheaderslist":<String_value>,
```

```
"additionalrespheaderslist":<String_value>,

"onlytransformabsurlinbody":<String_value>,

"comment":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/transformprofile? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "transformprofile": [ { "__count": "#no"} ] }
```

transformprofile_binding

Binding object which returns the resources bound to transformprofile.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the profile. Minimum length = 1
transformprofile_transformaction_binding	<transformprofile_transformaction_binding[]>	Read-only	transformaction that can be bound to transformprofile.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/transformprofile_binding/ name_value<String>
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "transformprofile_binding": [ {

"name":<String_value>,

"transformprofile_transformaction_binding":<transformprofile_transformacti
on_binding[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/transformprofile_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ transformprofile_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "transformprofile_binding": [ {

"name":<String_value>,

"transformprofile_transformaction_binding":<transformprofile_transformacti
on_binding[]_value>

}]}
```

transformprofile_transformaction_binding

Binding object showing the transformaction that can be bound to transformprofile.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the profile. Minimum length = 1
actionname	<String>	Read-write	URL Transformation action name.
requrlinto	<String>	Read-only	Pattern of transformed request URLs. It corresponds to internal addresses

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			and indicates how they are created.
actioncomment	<String>	Read-only	Comments.
cookiedomainfrom	<String>	Read-only	Pattern of the original domain in Set-Cookie headers.
resurlfrom	<String>	Read-only	Pattern of original response URLs. It corresponds to the way external users view the server, and acts as a source for response transformations.
cookiedomaininto	<String>	Read-only	Pattern of the transformed domain in Set-Cookie headers.
profilename	<String>	Read-only	URL Transformation profile name.
requrlfrom	<String>	Read-only	Pattern of original request URLs. It corresponds to the way external users view the server, and acts as a source for request transformations.
resurlinto	<String>	Read-only	Pattern of transformed response URLs. It corresponds to internal addresses

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			and indicates how they are created.
priority	<Integer>	Read-only	Priority of the Action within the Profile.
state	<String>	Read-only	Enabled flag. Possible values = ENABLED, DISABLED
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/transformprofile_transformaction_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ transformprofile_transformaction_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of transformprofile_transformaction_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ transformprofile_transformaction_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the transformprofile_transformaction_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "transformprofile_transformaction_binding": [ {

"name":<String_value>,
```

```
"actionname":<String_value>,

"requrlinto":<String_value>,

"actioncomment":<String_value>,

"cookiedomainfrom":<String_value>,

"resurlfrom":<String_value>,

"cookiedomaininto":<String_value>,

"profilename":<String_value>,

"requrlfrom":<String_value>,

"resurlinto":<String_value>,

"priority":<Integer_value>,

"state":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/transformprofile_transformaction_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/transformprofile_transformaction_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "transformprofile_transformaction_binding": [ {

"name":<String_value>,

"actionname":<String_value>,

"requrlinto":<String_value>,

"actioncomment":<String_value>,

"cookiedomainfrom":<String_value>,

"resurlfrom":<String_value>,

"cookiedomaininto":<String_value>,

"profilename":<String_value>,

"requrlfrom":<String_value>,

"resurlinto":<String_value>,

"priority":<Integer_value>,

"state":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/transformprofile_transformaction_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"transformprofile_transformaction_binding": [ { "__count": "#no"} ] }
```

tunnel

Tunnel

SSL VPN Tunnel Configuration.

NAME	DESCRIPTION
tunnelglobal_binding	Binding object showing the resources that can be bound to tunnelglobal
tunnelglobal_tunneltrafficpolicy_binding	Binding object showing the tunneltrafficpolicy that can be bound to tunnelglobal
tunneltrafficpolicy	Configuration for tunnel policy
tunneltrafficpolicy_binding	Binding object showing the resources that can be bound to tunneltrafficpolicy
tunneltrafficpolicy_tunnelglobal_binding	Binding object showing the tunnelglobal that can be bound to tunneltrafficpolicy

NAME	DESCRIPTION

tunnelglobal_binding

Binding object which returns the resources bound to tunnelglobal.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
tunnelglobal_tunneltrafficpolicy_binding	<tunnelglobal_tunneltrafficpolicy_binding[]>	Read-write	tunneltrafficpolicy that can be bound to tunnelglobal.

Operations

(click to see Properties)

- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/tunnelglobal_binding

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "tunnelglobal_binding": [ {

"tunnelglobal_tunneltrafficpolicy_binding":<tunnelglobal_tunneltrafficpoli
cy_binding[]_value>

}]}
```

tunnelglobal_tunneltrafficpolicy_binding

Binding object showing the tunneltrafficpolicy that can be bound to tunnelglobal.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
feature	<String>	Read-write	The feature to be checked while applying this config.
gotopriorityexpression	<String>	Read-write	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
policyname	<String>	Read-write	Policy name.
globalbindtype	<String>	Read-write	. Default value: SYSTEM_GLOBAL Possible values = SYSTEM_GLOBAL, VPN_GLOBAL, RNAT_GLOBAL, APPFW_GLOBAL, TM_GLOBAL
type	<String>	Read-write	Bind point to which the policy is bound. Possible values = REQ_OVERRIDE, REQ_DEFAULT, RES_OVERRIDE, RES_DEFAULT
builtin	<String[]>	Read-write	Indicates that a variable is a built-in

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			(SYSTEM INTERNAL) type. Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL
state	<String>	Read-write	Current state of the binding. If the binding is enabled, the policy is active. Possible values = ENABLED, DISABLED
priority	<Integer>	Read-write	Priority.
policytype	<String>	Read-only	Policy type (Classic/ Advanced) to be bound.Used for display. Possible values = Classic Policy, Advanced Policy
numpol	<Integer>	Read-only	The number of policies bound to the bindpoint.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET

- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/tunnelglobal_tunneltrafficpolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"tunnelglobal_tunneltrafficpolicy_binding":{

<b>"policyname":<String_value>,

</b>"priority":<Integer_value>,

"gotopriorityexpression":<String_value>,

"state":<String_value>,

"type":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/tunnelglobal_tunneltrafficpolicy_binding **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/tunnelglobal_tunneltrafficpolicy_binding? **args= policyname:<String_value>, type: <String_value> ,priority: <Integer_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/tunnelglobal_tunneltrafficpolicy_binding **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/tunnelglobal_tunneltrafficpolicy_binding? **args=type: <String_value>**

Use this query-parameter to get tunnelglobal_tunneltrafficpolicy_binding resources based on additional properties.

filter http:// <netscaler-ip-address> /nitro/v1/config/tunnelglobal_tunneltrafficpolicy_binding? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of tunnelglobal_tunneltrafficpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/tunnelglobal_tunneltrafficpolicy_binding? **pagesize=#no;pageno=#no**

Use this query-parameter to get the tunnelglobal_tunneltrafficpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "tunnelglobal_tunneltrafficpolicy_binding": [ {

"feature":<String_value>,

"gotopriorityexpression":<String_value>,
```

```
"policyname":<String_value>,

"globalbindtype":<String_value>,

"type":<String_value>,

"builtin":<String[]_value>,

"state":<String_value>,

"priority":<Integer_value>,

"policytype":<String_value>,

"numpol":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/tunnelglobal_tunneltrafficpolicy_binding?**count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "tunnelglobal_tunneltrafficpolicy_binding": [ { "__count": "#no"} ] }
```

tunneltrafficpolicy

Configuration for tunnel policy resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the tunnel traffic policy. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the policy is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			"my policy" or 'my policy)'. Minimum length = 1
rule	<String>	Read-write	Expression, against which traffic is evaluated. The following requirements apply only to the Citrix ADC CLI: * If the expression includes blank spaces, the entire expression must be enclosed in double quotation marks. * If the expression itself includes double quotation marks, you must escape the quotations by using the \ character. * Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
action	<String>	Read-write	Name of the built-in compression action to associate with the policy. Minimum length = 1
comment	<String>	Read-write	Any comments to preserve information about this policy.
logaction	<String>	Read-write	Name of the messagelog action to use for requests that match this policy.
newname	<String>	Read-write	New name for the tunnel traffic policy. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), e quals (=), and hyphen (-) characters. Choose a name that reflects the function that the policy performs. The following requirement applies only to the Citrix ADC CLI:

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my tunnel policy" or 'my tunnel policy'). Minimum length = 1
expressiontype	<String>	Read-only	Type of policy (Classic/Advanced). Possible values = Classic Policy, Advanced Policy
hits	<Integer>	Read-only	No of hits.
undefhits	<Integer>	Read-only	Number of policy UNDEF hits.
txbytes	<Integer>	Read-only	Number of bytes transmitted.
rxbytes	<Integer>	Read-only	Number of bytes received.
clientttlb	<Integer>	Read-only	Total client TTLB value.
clienttransactions	<Integer>	Read-only	Number of client transactions.
serverttlb	<Integer>	Read-only	Total server TTLB value.
servertransactions	<Integer>	Read-only	Number of server transactions.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
isdefault	<Boolean>	Read-only	A value of true is returned if it is a default tunnelpolicy.
builtin	<String[]>	Read-only	Indicates that a variable is a built-in (SYSTEM INTERNAL) type. Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL
feature	<String>	Read-only	The feature to be checked while applying this config.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT
- RENAME

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/tunneltrafficpolicy **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"tunneltrafficpolicy":{

<b>"name":<String_value>,

</b><b>"rule":<String_value>,

</b><b>"action":<String_value>,
```

```
</b>"comment":<String_value>,

"logaction":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/tunneltrafficpolicy/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/tunneltrafficpolicy **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"tunneltrafficpolicy":{

<b>"name":<String_value>,

</b>"rule":<String_value>,

"action":<String_value>,
```

```
"comment":<String_value>,

"logaction":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/tunneltrafficpolicy? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"tunneltrafficpolicy":{

<b>"name":<String_value>,

</b>"comment":true,

"logaction":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

RENAME

URL: http:// <netscaler-ip-address> /nitro/v1/config/tunneltrafficpolicy? **action=rename HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"tunneltrafficpolicy":{

<b>"name":<String_value>,

</b><b>"newname":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/tunneltrafficpolicy **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/tunneltrafficpolicy? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/tunneltrafficpolicy? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of tunneltrafficpolicy resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/tunneltrafficpolicy? **view=summary**

Use this query-parameter to get the summary output of tunneltrafficpolicy resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/tunneltrafficpolicy? **pagesize=#no;pageno=#no**

Use this query-parameter to get the tunneltrafficpolicy resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "tunneltrafficpolicy": [ {

"name":<String_value>,

"expressiontype":<String_value>,

"rule":<String_value>,

"action":<String_value>,

"hits":<Integer_value>,

"undefhits":<Integer_value>,

"txbytes":<Integer_value>,

"rxbytes":<Integer_value>,

"clientttlb":<Integer_value>,
```

```
"clienttransactions":<Integer_value>,

"serverttlb":<Integer_value>,

"servertransactions":<Integer_value>,

"comment":<String_value>,

"logaction":<String_value>,

"isdefault":<Boolean_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/tunneltrafficpolicy/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/tunneltrafficpolicy/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/tunneltrafficpolicy/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of tunneltrafficpolicy resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "tunneltrafficpolicy": [ {

"name":<String_value>,

"expressiontype":<String_value>,

"rule":<String_value>,

"action":<String_value>,

"hits":<Integer_value>,

"undefhits":<Integer_value>,

"txbytes":<Integer_value>,

"rxbytes":<Integer_value>,

"clientttlb":<Integer_value>,

"clienttransactions":<Integer_value>,

"serverttlb":<Integer_value>,

"servertransactions":<Integer_value>,

"comment":<String_value>,

"logaction":<String_value>,

"isdefault":<Boolean_value>,

"builtin":<String[]_value>,
```

```
"feature":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/tunneltrafficpolicy? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "tunneltrafficpolicy": [ { "__count": "#no"} ] }
```

tunneltrafficpolicy_binding

Binding object which returns the resources bound to tunneltrafficpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the tunnel traffic policy for

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			which to show detailed information. Minimum length = 1
tunneltrafficpolicy_tunnelglobal_binding	<tunneltrafficpolicy_tunnelglobal_binding[]>	Read-only	tunnelglobal that can be bound to tunneltrafficpolicy.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/tunneltrafficpolicy_binding/ name_value<String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "tunneltrafficpolicy_binding": [ {

"name":<String_value>,

"tunneltrafficpolicy_tunnelglobal_binding":<tunneltrafficpolicy_tunnelglob
al_binding[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/tunneltrafficpolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ tunneltrafficpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "tunneltrafficpolicy_binding": [ {

"name":<String_value>,

"tunneltrafficpolicy_tunnelglobal_binding":<tunneltrafficpolicy_tunnelglob
al_binding[]_value>

}]}
```

tunneltrafficpolicy_tunnelglobal_binding

Binding object showing the tunnelglobal that can be bound to tunneltrafficpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the tunnel traffic policy for which to show detailed information. Minimum length = 1
boundto	<String>	Read-write	The entity name to which policy is bound.
priority	<Integer>	Read-only	.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
activepolicy	<Integer>	Read-only	.
gotopriorityexpression	<String>	Read-only	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/tunneltrafficpolicy_tunnelglobal_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ tunneltrafficpolicy_tunnelglobal_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of tunneltrafficpolicy_tunnelglobal_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/tunneltrafficpolicy_tunnelglobal_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the tunneltrafficpolicy_tunnelglobal_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "tunneltrafficpolicy_tunnelglobal_binding": [ {

"name":<String_value>,
```

```
"boundto":<String_value>,

"priority":<Integer_value>,

"activepolicy":<Integer_value>,

"gotopriorityexpression":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/tunneltrafficpolicy_tunnelglobal_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/tunneltrafficpolicy_tunnelglobal_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "tunneltrafficpolicy_tunnelglobal_binding": [ {

"name":<String_value>,
```

```
"boundto":<String_value>,

"priority":<Integer_value>,

"activepolicy":<Integer_value>,

"gotopriorityexpression":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/tunneltrafficpolicy_tunnelglobal_binding/name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"tunneltrafficpolicy_tunnelglobal_binding": [ { "__count": "#no"} ] }
```

ulfd

Ulfd

ULFD server configuration.

NAME	DESCRIPTION
ulfdserver	Configuration for ulfd server

ulfdserver

Configuration for ulfd server resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
loggerip	<String>	Read-write	IP address of the server where ulfd service is running. Minimum length = 1
state	<String>	Read-only	ULFD server state. Possible values = UP, DOWN, UNKNOWN, BUSY, OUT OF SERVICE, GOING OUT OF SERVICE, DOWN WHEN GOING OUT OF SERVICE, NS_EMPTY_STR, Unknown, DISABLED
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD

- DELETE
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/ulfdserver **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"ulfdserver":{

<b>"loggerip":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/ulfdserver/ loggerip_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/ulfdserver **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/ulfdserver? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/ulfdserver? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of ulfdserver resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/ulfdserver? **view=summary**

Use this query-parameter to get the summary output of ulfdserver resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/ulfdserver? **pagesize=#no;pageno=#no**

Use this query-parameter to get the ulfdserver resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "ulfdserver": [ {

"loggerip":<String_value>,

"state":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/ulfdserver/ loggerip_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/ulfdserver/ loggerip_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/ulfdserver/ loggerip_value<String> ? **view=summary**

Use this query-parameter to get the summary output of ulfdserver resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "ulfdserver": [ {

"loggerip":<String_value>,

"state":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/ulfdserver? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "ulfdserver": [ { "__count": "#no"} ] }
```

user

User

User protocol configuration.

NAME	DESCRIPTION
userprotocol	Configuration for user protocol
uservserver	Configuration for virtual server

userprotocol

Configuration for user protocol resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Unique name for the user protocol. Not case sensitive. Must begin with an ASCII letter or underscore (_) character, and

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			must consist only of ASCII alphanumeric or underscore characters. Minimum length = 1
transport	<String>	Read-write	Transport layer's protocol. Possible values = TCP, SSL
extension	<String>	Read-write	Name of the extension to add parsing and runtime handling of the protocol packets.
wasmmodule	<String>	Read-write	Wasm module needs to attach with the user protocol.
comment	<String>	Read-write	Any comments associated with the protocol.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET

- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/userprotocol **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"userprotocol":{

<b>"name":<String_value>,
```

```
</b><b>"transport":<String_value>,

</b>"extension":<String_value>,

"wasmmodule":<String_value>,

"comment":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/userprotocol/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/userprotocol **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"userprotocol":{

<b>"name":<String_value>,
```

```
</b>"comment":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/userprotocol? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"userprotocol":{

<b>"name":<String_value>,

</b>"comment":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/userprotocol **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/userprotocol? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/userprotocol? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of userprotocol resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/userprotocol? **view=summary**

Use this query-parameter to get the summary output of userprotocol resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/userprotocol? **pagesize=#no;pageno=#no**

Use this query-parameter to get the userprotocol resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "userprotocol": [ {

"name":<String_value>,

"transport":<String_value>,

"extension":<String_value>,
```

```
"wasmmodule":<String_value>,

"comment":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/userprotocol/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/userprotocol/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/userprotocol/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of userprotocol resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "userprotocol": [ {

"name":<String_value>,

"transport":<String_value>,

"extension":<String_value>,

"wasmmodule":<String_value>,

"comment":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/userprotocol? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "userprotocol": [ { "__count": "#no"} ] }
```

uservserver

Configuration for virtual server resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the virtual server. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at sign (@), equal sign (=), and hyphen (-) characters. CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my vserver" or 'my vserver'). . Minimum length = 1
userprotocol	<String>	Read-write	User protocol uesd by the service.
ipaddress	<String>	Read-write	IPv4 or IPv6 address to assign to the virtual server.
port	<Integer>	Read-write	Port number for the virtual server.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Range 1 - 65535 * in CLI is represented as 65535 in NITRO API
defaultlb	<String>	Read-write	Name of the default Load Balancing virtual server used for load balancing of services. The protocol type of default Load Balancing virtual server should be a user type.
Params	<String>	Read-write	Any comments associated with the protocol.
comment	<String>	Read-write	Any comments that you might want to associate with the virtual server.
state	<String>	Read-write	Initial state of the user vserver. Default value: ENABLED Possible values = ENABLED, DISABLED
curstate	<String>	Read-only	Current user vserver state. Possible values = UP, DOWN,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			UNKNOWN, BUSY, OUT OF SERVICE, GOING OUT OF SERVICE, DOWN WHEN GOING OUT OF SERVICE, NS_EMPTY_STR, Unknown, DISABLED
value	<String>	Read-only	SSL status. Possible values = Certkey/ Certkeybundle/Vault not bound/Cert-store not usable, SSL feature disabled
statechangetimesec	<String>	Read-only	Time when last state change happened. Seconds part.
statechangetimemsec	<Integer>	Read-only	Time at which last state change happened. Milliseconds part.
tickssincelaststatechange	<Integer>	Read-only	Time in 10 millisecond ticks since the last state change.
nodefaultbindings	<String>	Read-only	to determine if the configuration will have default ssl CIPHER and ECC curve bindings.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: NO Possible values = YES, NO
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- ENABLE
- DISABLE
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/uservserver **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"uservserver":{

<b>"name":<String_value>,

</b><b>"userprotocol":<String_value>,

</b><b>"ipaddress":<String_value>,

</b><b>"port":<Integer_value>,

</b><b>"defaultlb":<String_value>,

</b>"Params":<String_value>,

"comment":<String_value>,

"state":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/uservserver/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/uservserver **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"uservserver":{

<b>"name":<String_value>,

</b>"ipaddress":<String_value>,

"defaultlb":<String_value>,

"Params":<String_value>,

"comment":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/uservserver? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"uservserver":{

<b>"name":<String_value>,

</b>"Params":true,

"comment":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

ENABLE

URL: http:// <netscaler-ip-address> /nitro/v1/config/uservserver? **action=enable HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"uservserver":{

<b>"name":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DISABLE

URL: http:// <netscaler-ip-address> /nitro/v1/config/uservserver? **action=disable HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"uservserver":{

<b>"name":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/uservserver **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/uservserver? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/uservserver? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of uservserver resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/uservserver? **view=summary**

Use this query-parameter to get the summary output of uservserver resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/uservserver? **pagesize=#no;pageno=#no**

Use this query-parameter to get the uservserver resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "uservserver": [ {

"name":<String_value>,

"userprotocol":<String_value>,

"ipaddress":<String_value>,

"port":<Integer_value>,

"defaultlb":<String_value>,

"Params":<String_value>,

"comment":<String_value>,

"curstate":<String_value>,

"value":<String_value>,

"statechangetimesec":<String_value>,

"statechangetimemsec":<Integer_value>,

"tickssincelaststatechange":<Integer_value>,

"state":<String_value>,

"nodefaultbindings":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/uservserver/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/uservserver/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/uservserver/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of uservserver resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "uservserver": [ {

"name":<String_value>,

"userprotocol":<String_value>,

"ipaddress":<String_value>,

"port":<Integer_value>,

"defaultlb":<String_value>,

"Params":<String_value>,

"comment":<String_value>,

"curstate":<String_value>,
```

```
"value":<String_value>,

"statechangetimesec":<String_value>,

"statechangetimemsec":<Integer_value>,

"tickssincelaststatechange":<Integer_value>,

"state":<String_value>,

"nodefaultbindings":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/uservserver? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "uservserver": [ { "__count": "#no"} ] }
```

utility

Utility

Utilities.

NAME	DESCRIPTION
callhome	Configuration for callhome
filesystemencryption	Configuration for File System Encryption Information
install	
ping	
ping6	
raid	Configuration for raid support
techsupport	Configuration for tech support
traceroute	
traceroute6	

callhome

Configuration for callhome resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
nodeid	<Integer>	Read-write	Unique number that identifies the cluster node. Minimum value = 0 Maximum value = 31

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
mode	<String>	Read-write	CallHome mode of operation. Default value: Default Possible values = Default, CSP, Connector
emailaddress	<String>	Read-write	Email address of the contact administrator. Maximum length = 78
hbcustominterval	<Integer>	Read-write	Interval (in days) between CallHome heartbeats. Default value: 7 Minimum value = 1 Maximum value = 30
proxymode	<String>	Read-write	Enables or disables the proxy mode. The proxy server can be set by either specifying the IP address of the server or the name of the service representing the proxy server. Default value: NO Possible values = YES, NO

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ipaddress	<String>	Read-write	IP address of the proxy server. Minimum length = 1
proxyauthservice	<String>	Read-write	Name of the service that represents the proxy server. Maximum length = 128
port	<Integer>	Read-write	HTTP port on the Proxy server. This is a mandatory parameter for both IP address and service name based configuration. Minimum value = 1 Range 1 - 65535 * in CLI is represented as 65535 in NITRO API
sslcardfirstfailure	<String>	Read-only	First occurrence SSL card failure.
sslcardlatestfailure	<String>	Read-only	Latest occurrence SSL card failure.
powfirstfail	<String>	Read-only	First occurrence power supply unit failure.
powlatestfailure	<String>	Read-only	Latest occurrence power supply unit failure.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
hddfirstfail	<String>	Read-only	First occurrence hard disk drive failure.
hddlatestfailure	<String>	Read-only	Latest occurrence hard disk drive failure.
flashfirstfail	<String>	Read-only	First occurrence compact flash failure.
flashlatestfailure	<String>	Read-only	Latest occurrence compact flush failure.
rlfirsthighdrop	<String>	Read-only	First occurence of high rate limit drops.
rllatesthighdrop	<String>	Read-only	Latest occurence of high rate limit drops.
restartlatestfail	<String>	Read-only	Latest occurrence warm restart failure.
memthrefirstanomaly	<String>	Read-only	First occurrence of memory anomaly.
memthrelatestanomaly	<String>	Read-only	Latest occurrence of memory anomaly.
callhomestatus	<String[]>	Read-only	Callhome feature enabled/disable, register with upload server successful/ failed. Possible values = ENABLED, DISABLED, SUCCESSFUL, FAILED, INVALID HOSTNAME, NO DNSSERVER,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			HOSTNAME RESOLUTION FAILED
anomalydetection	<String>	Read-only	Enables or disables anomaly detection. Default value: DISABLED Possible values = ENABLED, DISABLED
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- GET (ALL)
- UPDATE
- UNSET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/callhome **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"callhome":{

"mode":<String_value>,

"emailaddress":<String_value>,

"hbcustominterval":<Integer_value>,

"proxymode":<String_value>,

"ipaddress":<String_value>,

"proxyauthservice":<String_value>,

"port":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/callhome? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"callhome":{

"mode":true,

"emailaddress":true,

"hbcustominterval":true,

"proxymode":true,

"ipaddress":true,

"proxyauthservice":true,

"port":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/callhome **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/callhome? **args=nodeid: <Integer_value>**

Use this query-parameter to get callhome resources based on additional properties.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "callhome": [ {

nodeid:<Integer_value>"mode":<String_value>,

"emailaddress":<String_value>,

"hbcustominterval":<Integer_value>,

"proxymode":<String_value>,

"ipaddress":<String_value>,

"port":<Integer_value>,

"proxyauthservice":<String_value>,

"sslcardfirstfailure":<String_value>,

"sslcardlatestfailure":<String_value>,

"powfirstfail":<String_value>,

"powlatestfailure":<String_value>,

"hddfirstfail":<String_value>,

"hddlatestfailure":<String_value>,
```

```
"flashfirstfail":<String_value>,

"flashlatestfailure":<String_value>,

"rlfirsthighdrop":<String_value>,

"rllatesthighdrop":<String_value>,

"restartlatestfail":<String_value>,

"memthrefirstanomaly":<String_value>,

"memthrelatestanomaly":<String_value>,

"callhomestatus":<String[]_value>,

"anomalydetection":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

filesystemencryption

Configuration for File System Encryption Information resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ntimes0flash	<Integer>	Read-write	Number of times / flash directory has to be written with 0s. Default value: 0 Minimum value = 0 Maximum value = 16

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ntimes0var	<Integer>	Read-write	Number of times /var directory has to be written with 0s. Default value: 0 Minimum value = 0 Maximum value = 16
passphrase	<String>	Read-write	Encryption Passphrase. Minimum length = 1 Maximum length = 512
nodeid	<Integer>	Read-write	Unique number that identifies the cluster node. Minimum value = 0 Maximum value = 31
supportedstate	<String>	Read-only	Get the supported state of File System Encryption. Default value: 0 Possible values = DISABLED, ENABLED, ELIGIBLE
effectivestate	<String>	Read-only	Get the current encrypted state of the File System.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ENABLED, DISABLED
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- ENABLE
- DISABLE
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ENABLE

URL: http:// <netscaler-ip-address> /nitro/v1/config/filesystemencryption? **action=enable HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"filesystemencryption":{

<b>"ntimes0flash":<Integer_value>,

</b><b>"ntimes0var":<Integer_value>,

</b><b>"passphrase":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DISABLE

URL: http:// <netscaler-ip-address> /nitro/v1/config/filesystemencryption? **action=disable HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"filesystemencryption":{

<b>"ntimes0flash":<Integer_value>,
```

```
</b><b>"ntimes0var":<Integer_value>,

</b><b>"passphrase":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/filesystemencryption **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/filesystemencryption? **args=nodeid: <Integer_value>**

Use this query-parameter to get filesystemencryption resources based on additional properties.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "filesystemencryption": [ {

nodeid:<Integer_value>"supportedstate":<String_value>,

"effectivestate":<String_value>,
```

```
"_nextgenapiresource":<String_value>

}]}
```

install

Configuration for 0 resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
url	<String>	Read-write	Url for the build file. Must be in the following formats: http://[user]:[password]@host/path/to/file https://[user]:[password]@host/path/to/file sftp://[user]:[password]@host/path/to/file scp://[user]:[password]@host/path/to/file ftp://[user]:[password]@host/path/to/file file://path/to/file.
Async	<Boolean>	Read-write	Use this flag to return the install id

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			when the nitro api request is sent. The id can be used later to track the installation progress via show ns job <id> command. For the cli request of install the flag is by default set as false as the installation progress details can be tracked via cli.
y	<Boolean>	Read-write	Do not prompt for yes/no before rebooting.
l	<Boolean>	Read-write	Use this flag to enable callhome.
a	<Boolean>	Read-write	Use this flag to enable Citrix ADM Service Connect. This feature helps you discover your Citrix ADC instances effortlessly on Citrix ADM service and get insights and curated machine learning based recommendations for applications and Citrix ADC infrastructure. This feature lets the Citrix ADC instance

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			automatically send system, usage and telemetry data to Citrix ADM service. View here [https://docs.citrix.com/en-us/citrix-adc/13/data-governance.html] to learn more about this feature. Use of this feature is subject to the Citrix End User ServiceAgreement. View here [https://www.citrix.com/buy/licensing/agreements.html].
fipsinstall	<Boolean>	Read-write	Use this flag to perform FIPS installation.
answeryestoall	<Boolean>	Read-write	Use this flag to answer yes to all prompts.
dontreboot	<Boolean>	Read-write	Use this flag to prevent reboot after installation when answerYesToAll is true.
dontchecknsconf	<Boolean>	Read-write	Use this flag to skip ns.conf version equivalence check during downgrade.
deletesigfiles	<Boolean>	Read-write	Use this flag to delete all signature files and associated

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			kernel images during installation.
ignorensapimgrerrors	<Boolean>	Read-write	Use this flag to ignore nsapimgr symbols not found error(s) during installation.
exitonlicserverconnerror	<Boolean>	Read-write	Use this flag to exit on license server connectivity errors.
precheck	<Boolean>	Read-write	Use this flag to run all installation pre-checks in a single step.
advancedoptions	<String>	Read-write	Use this string to pass extra flags which are not yet supported. Example: -flag1 -flag2 -flag3.
ignoreunsavedconfig	<Boolean>	Read-write	Use this flag to ignore unsaved config check during build update.
ignoreunsyncedconfig	<Boolean>	Read-write	Use this flag to ignore unsynced HA config check during build update.
ignorecertcheckerrors	<Boolean>	Read-write	Use this flag to ignore certificate digest verification errors during build update.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
id	<Integer>	Read-only	Job Id for install process.

Operations

(click to see Properties)

- INSTALL

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

INSTALL

URL: http:// <netscaler-ip-address> /nitro/v1/config/install **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"install":{

<b>"url":<String_value>,

</b>"Async":<Boolean_value>,

"y":<Boolean_value>,

"l":<Boolean_value>,

"a":<Boolean_value>,

"fipsinstall":<Boolean_value>,

"answeryestoall":<Boolean_value>,

"dontreboot":<Boolean_value>,

"dontchecknsconf":<Boolean_value>,

"deletesigfiles":<Boolean_value>,

"ignorensapimgrerrors":<Boolean_value>,

"exitonlicserverconnerror":<Boolean_value>,

"precheck":<Boolean_value>,

"advancedoptions":<String_value>,

"ignoreunsavedconfig":<Boolean_value>,

"ignoreunsyncedconfig":<Boolean_value>,

"ignorecertcheckerrors":<Boolean_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Payload:

```
{ "install": [ {

"id":<Integer_value>



}]}
```

ping

Configuration for 0 resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
c	<Integer>	Read-write	Number of packets to send. The default value is infinite. For Nitro API, defalut value is taken as 5. Minimum value = 1 Maximum value = 65535
i	<Integer>	Read-write	Waiting time, in seconds. The default value is 1 second. Minimum value = 0

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum value = 65535
I	<String>	Read-write	Network interface on which to ping, if you have multiple interfaces. Minimum length = 1 Maximum length = 15
n	<Boolean>	Read-write	Numeric output only. No name resolution.
p	<String>	Read-write	Pattern to fill in packets. Can be up to 16 bytes, useful for diagnosing data-dependent problems. Minimum length = 1 Maximum length = 32
q	<Boolean>	Read-write	Quiet output. Only the summary is printed. For Nitro API, this flag is set by default.
s	<Integer>	Read-write	Data size, in bytes. The default value is 56. Minimum value = 0 Maximum value = 65507
S	<String>	Read-write	Source IP address to be used in the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			outgoing query packets. If the IP addrESS does not belongs to this appliance, an error is returned and nothing is sent. Minimum length = 1
T	<Integer>	Read-write	Traffic Domain Id. Minimum value = 1 Maximum value = 4094
t	<Integer>	Read-write	Time-out, in seconds, before ping exits. Minimum value = 1 Maximum value = 3600
hostName	<String>	Read-write	Address of host to ping. Minimum length = 1 Maximum length = 256
response	<String>	Read-only	.

Operations

(click to see Properties)

- PING

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

PING

URL: http:// <netscaler-ip-address> /nitro/v1/config/ping **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"ping":{

"c":<Integer_value>,

"i":<Integer_value>,

"I":<String_value>,
```

```
"n":<Boolean_value>,

"p":<String_value>,

"q":<Boolean_value>,

"s":<Integer_value>,

"S":<String_value>,

"T":<Integer_value>,

"t":<Integer_value>,

<b>"hostName":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Payload:

```
{ "ping": [ {

"response":<String_value>



}]}
```

ping6

Configuration for 0 resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
b	<Integer>	Read-write	Set socket buffer size. If used, should be used with roughly +100 then the datalen (-s option). The default value is 8192. Minimum value = 132 Maximum value = 131071
c	<Integer>	Read-write	Number of packets to send. The default value is infinite. For Nitro API, defalut value is taken as 5. Minimum value = 1 Maximum value = 65535
i	<Integer>	Read-write	Waiting time, in seconds. The default value is 1 second. Minimum value = 0 Maximum value = 65535
I	<String>	Read-write	Network interface on which to ping, if you have multiple interfaces. Minimum length = 1 Maximum length = 15

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
m	<Boolean>	Read-write	By default, ping6 asks the kernel to fragment packets to fit into the minimum IPv6 MTU.The -m option will suppress the behavior for unicast packets.
n	<Boolean>	Read-write	Numeric output only. No name resolution.
p	<String>	Read-write	Pattern to fill in packets. Can be up to 16 bytes, useful for diagnosing data-dependent problems. Minimum length = 1 Maximum length = 32
q	<Boolean>	Read-write	Quiet output. Only summary is printed. For Nitro API, this flag is set by default.
s	<Integer>	Read-write	Data size, in bytes. The default value is 32. Minimum value = 0 Maximum value = 65527
V	<Integer>	Read-write	VLAN ID for link local address. Minimum value = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum value = 4094
S	<String>	Read-write	Source IP address to be used in the outgoing query packets. Minimum length = 1
T	<Integer>	Read-write	Traffic Domain Id. Minimum value = 1 Maximum value = 4094
t	<Integer>	Read-write	Timeout in seconds before ping6 exits.
hostName	<String>	Read-write	Address of host to ping. Minimum length = 1 Maximum length = 256
response	<String>	Read-only	.

Operations

(click to see Properties)

- PING6

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

PING6

URL: http:// <netscaler-ip-address> /nitro/v1/config/ping6 **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"ping6":{

"b":<Integer_value>,

"c":<Integer_value>,

"i":<Integer_value>,

"I":<String_value>,

"m":<Boolean_value>,

"n":<Boolean_value>,
```

```
"p":<String_value>,

"q":<Boolean_value>,

"s":<Integer_value>,

"V":<Integer_value>,

"S":<String_value>,

"T":<Integer_value>,

"t":<Integer_value>,

<b>"hostName":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Payload:

```
{ "ping6": [ {

"response":<String_value>



}]}
```

raid

Configuration for raid support resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
_nextgenapiresource	<String>	Read-write	.

Operations

(click to see Properties)

- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/raid

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "raid": [ {

"_nextgenapiresource":<String_value>

}]}
```

techsupport

Configuration for tech support resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
scope	<String>	Read-write	Use this option to gather data on the present node, all cluster nodes, or for the specified partitions. The CLUSTER scope generates smaller abbreviated archives

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			for all nodes. The PARTITION scope collects the admin partition in addition to those specified. The partitionName option is only required for the PARTITION scope. Default value: NODE Possible values = NODE, CLUSTER, PARTITION
partitionname	<String>	Read-write	Name of the partition. Minimum length = 1
upload	<Boolean>	Read-write	Securely upload the collector archive to Citrix Technical Support using SSL. MyCitrix credentials will be required. If used with the -file option, no new collector archive is generated. Instead, the specified archive is uploaded. Note that the upload operation time depends on the size of the archive file, and the connection bandwidth.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
proxy	<String>	Read-write	Specifies the proxy server to be used when uploading a collector archive. Use this parameter if the Citrix ADC does not have direct internet connectivity. The basic format of the proxy string is: "proxy_IP:<proxy_port>" (without quotes). If the proxy requires authentication the format is: "username:password@proxy_IP:<proxy_port>".
casenumber	<String>	Read-write	Specifies the associated case or service request number if it has already been opened with Citrix Technical Support.
file	<String>	Read-write	Specifies the name (with full path) of the collector archive file to be uploaded. If this is specified, no new collector archive is generated.
description	<String>	Read-write	Provides a text description for the the upload, and can be used for logging purposes.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
authtoken	<String>	Read-write	Specifies the Authentication Token, which is used to login to Citrix upload server. Please copy/paste the URL https://cis.citrix.com/auth/api/create_identity_v2/?expiration=3600 in a browser to complete the two factor authentication and generate it. The token is valid for 3600 seconds (1 hour).
time	<String>	Read-write	Specifies the time in common log format, ie. DD/MMM/YYYY:HH:MM:SS, to be used for locating the newnslog file. With this option at most four newnslog log files are collected. First is the newnslog file, spanning the given time. Second is the one, created just prior to the first (if it exists). Third is the one, created just later than the first (if it exists). And the fourth is the latest newnslog directory. In case, the scope is

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			cluster, then second and third type is skipped on all nodes. Minimum length = 20 Maximum length = 20
period	<Integer>	Read-write	Specifies the time window in hours around the time specified by -time option. This parameter is only valid when -time is specified. Defines the range for collecting newnslog files, text logs, and non-PE core files. For example, with -time "01/Jan/2026:12:00:00" and -period 2, logs and cores from 11:00:00 to 13:00:00 will be collected. Minimum value = 1
adss	<Boolean>	Read-write	Option for collecting showtechsupport bundle on ADSS cluster/node.
notruncate	<Boolean>	Read-write	Option for collecting showtechsupport bundle without truncating log files.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
nopecore	<Boolean>	Read-write	Option for collecting showtechsupport bundle without PE core files.
nodes	<Integer[]>	Read-write	Use this option to collect showtechsupport bundle only from the nodes given as a list to this option. If -file option is used, it will collect the files from the given nodes back to the cco and will upload the compressed folder containing the files from there. Minimum value = 0 Maximum value = 255
response	<String>	Read-only	Output as text printed to console and syslog at NOTICE level.
servername	<String>	Read-only	.
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/techsupport **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/techsupport? **args=scope: <String_value> ,partitionname: <String_value> ,upload: <Boolean_value> ,proxy: <String_value> ,casenumber: <String_value> ,file: <String_value> ,description: <String_value> ,authtoken: <String_value> ,time: <String_value> ,period: <Integer_value> ,adss: <Boolean_value> ,notruncate: <Boolean_value> ,nopecore: <Boolean_value> ,nodes: <Integer_value>**

Use this query-parameter to get techsupport resources based on additional properties.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "techsupport": [ {

scope:<String_value>,partitionname:<String_value>,upload:<Boolean_value>,p
roxy:<String_value>,casenumber:<String_value>,file:<String_value>,descript
ion:<String_value>,authtoken:<String_value>,time:<String_value>,period:<In
teger_value>,adss:<Boolean_value>,notruncate:<Boolean_value>,nopecore:<Boo
lean_value>,nodes:<Integer[]_value>"response":<String_value>,

"servername":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

traceroute

Configuration for 0 resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
S	<Boolean>	Read-write	Print a summary of how many probes were not answered for each hop.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
n	<Boolean>	Read-write	Print hop addresses numerically instead of symbolically and numerically.
r	<Boolean>	Read-write	Bypass normal routing tables and send directly to a host on an attached network. If the host is not on a directly attached network, an error is returned.
v	<Boolean>	Read-write	Verbose output. List received ICMP packets other than TIME_EXCEEDED and UNREACHABLE.
M	<Integer>	Read-write	Minimum TTL value used in outgoing probe packets. Default value: 1 Minimum value = 1 Maximum value = 255
m	<Integer>	Read-write	Maximum TTL value used in outgoing probe packets. For Nitro API, default value is taken as 10. Default value: 64 Minimum value = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum value = 255
P	<String>	Read-write	Send packets of specified IP protocol. The currently supported protocols are UDP and ICMP. Minimum length = 1 Maximum length = 20
p	<Integer>	Read-write	Base port number used in probes. Default value: 33434 Minimum value = 1 Maximum value = 65535
q	<Integer>	Read-write	Number of queries per hop. For Nitro API, defalut value is taken as 1. Default value: 3 Minimum value = 1 Maximum value = 65535
s	<String>	Read-write	Source IP address to use in the outgoing query packets. If the IP address does not belong to this appliance, an error is

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			returned and nothing is sent. Minimum length = 1
T	<Integer>	Read-write	Traffic Domain Id. Minimum value = 1 Maximum value = 4094
t	<Integer>	Read-write	Type-of-service in query packets. Minimum value = 0 Maximum value = 255
w	<Integer>	Read-write	Time (in seconds) to wait for a response to a query. For Nitro API, defalut value is set to 3. Default value: 5 Minimum value = 2 Maximum value = 86399
host	<String>	Read-write	Destination host IP address or name. Minimum length = 1 Maximum length = 64
packetlen	<Integer>	Read-write	Length (in bytes) of the query packets. Default value: 44

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum value = 44 Maximum value = 32768
response	<String>	Read-only	.

Operations

(click to see Properties)

- TRACEROUTE

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

TRACEROUTE

URL: http:// <netscaler-ip-address> /nitro/v1/config/traceroute **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"traceroute":{

"S":<Boolean_value>,

"n":<Boolean_value>,

"r":<Boolean_value>,

"v":<Boolean_value>,

"M":<Integer_value>,

"m":<Integer_value>,

"P":<String_value>,

"p":<Integer_value>,

"q":<Integer_value>,

"s":<String_value>,

"T":<Integer_value>,

"t":<Integer_value>,

"w":<Integer_value>,

<b>"host":<String_value>,

</b>"packetlen":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Payload:

```
{ "traceroute": [ {

"response":<String_value>



}]}
```

traceroute6

Configuration for 0 resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
n	<Boolean>	Read-write	Print hop addresses numerically rather than symbolically and numerically.
I	<Boolean>	Read-write	Use ICMP ECHO for probes.
r	<Boolean>	Read-write	Bypass normal routing tables and send directly to a host on an attached network. If the host is not on a directly

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			attached network, an error is returned.
v	<Boolean>	Read-write	Verbose output. List received ICMP packets other than TIME_EXCEEDED and UNREACHABLE.
m	<Integer>	Read-write	Maximum hop value for outgoing probe packets. For Nitro API, default value is taken as 10. Default value: 64 Minimum value = 1 Maximum value = 255
p	<Integer>	Read-write	Base port number used in probes. Default value: 33434 Minimum value = 1 Maximum value = 65535
q	<Integer>	Read-write	Number of probes per hop. For Nitro API, default value is taken as 1. Default value: 3 Minimum value = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum value = 65535
s	<String>	Read-write	Source IP address to use in the outgoing query packets. If the IP address does not belong to this appliance, an error is returned and nothing is sent. Minimum length = 1
T	<Integer>	Read-write	Traffic Domain Id. Minimum value = 1 Maximum value = 4094
w	<Integer>	Read-write	Time (in seconds) to wait for a response to a query. For Nitro API, defalut value is set to 3. Default value: 5 Minimum value = 2 Maximum value = 86399
host	<String>	Read-write	Destination host IP address or name. Minimum length = 1 Maximum length = 256
packetlen	<Integer>	Read-write	Length (in bytes) of the query packets.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: 44 Minimum value = 44 Maximum value = 32768
response	<String>	Read-only	.

Operations

(click to see Properties)

- TRACEROUTE6

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

TRACEROUTE6

URL: http:// <netscaler-ip-address> /nitro/v1/config/traceroute6 **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"traceroute6":{

"n":<Boolean_value>,

"I":<Boolean_value>,

"r":<Boolean_value>,

"v":<Boolean_value>,

"m":<Integer_value>,

"p":<Integer_value>,

"q":<Integer_value>,

"s":<String_value>,

"T":<Integer_value>,

"w":<Integer_value>,

<b>"host":<String_value>,

</b>"packetlen":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Payload:

```
{ "traceroute6": [ {

"response":<String_value>



}]}
```

videooptimization

VideoOptimization

Video optimization feature is used to show (i) the stats of different media types that are being served by the Citrix ADC and (ii) the details of optimization applied on ABR videos

NAME	DESCRIPTION
videooptimizationdetectionaction	Configuration for videooptimization detectionaction
videooptimizationdetectionpolicy	Configuration for videooptimization detectionpolicy
videooptimizationdetectionpolicy_binding	Binding object showing the resources that can be bound to videooptimizationdetectionpolicy
videooptimizationdetectionpolicy_lbvserver_binding	Binding object showing the lbvserver that can be bound to videooptimizationdetectionpolicy

NAME	DESCRIPTION
videooptimizationdetectionpolicy_videooptimizationglobaldetection_binding	Binding object showing the videooptimizationglobaldetection that can be bound to videooptimizationdetectionpolicy
videooptimizationdetectionpolicylabel	Configuration for videooptimization detection policy label
videooptimizationdetectionpolicylabel_binding	Binding object showing the resources that can be bound to videooptimizationdetectionpolicylabel
videooptimizationdetectionpolicylabel_policybinding_binding	Binding object showing the policybinding that can be bound to videooptimizationdetectionpolicylabel
videooptimizationdetectionpolicylabel_videooptimizationdetectionpolicy_binding	Binding object showing the videooptimizationdetectionpolicy that can be bound to videooptimizationdetectionpolicylabel
videooptimizationglobaldetection_binding	Binding object showing the resources that can be bound to videooptimizationglobaldetection
videooptimizationglobaldetection_videooptimizationdetectionpolicy_binding	Binding object showing the videooptimizationdetectionpolicy that can be bound to videooptimizationglobaldetection
videooptimizationglobalpacing_binding	Binding object showing the resources that can be bound to videooptimizationglobalpacing

NAME	DESCRIPTION
videooptimizationglobalpacing_videooptimizationpacingpolicy_binding	Binding object showing the videooptimizationpacingpolicy that can be bound to videooptimizationglobalpacing
videooptimizationpacingaction	Configuration for videooptimization pacingaction
videooptimizationpacingpolicy	Configuration for videooptimization pacingpolicy
videooptimizationpacingpolicy_binding	Binding object showing the resources that can be bound to videooptimizationpacingpolicy
videooptimizationpacingpolicy_lbvserver_binding	Binding object showing the lbvserver that can be bound to videooptimizationpacingpolicy
videooptimizationpacingpolicy_videooptimizationglobalpacing_binding	Binding object showing the videooptimizationglobalpacing that can be bound to videooptimizationpacingpolicy
videooptimizationpacingpolicylabel	Configuration for videooptimization pacing policy label
videooptimizationpacingpolicylabel_binding	Binding object showing the resources that can be bound to videooptimizationpacingpolicylabel
videooptimizationpacingpolicylabel_policybinding_binding	Binding object showing the policybinding that can be bound to videooptimizationpacingpolicylabel

NAME	DESCRIPTION
videooptimizationpacingpolicylabel_videooptimizationpacingpolicy_binding	Binding object showing the videooptimizationpacingpolicy that can be bound to videooptimizationpacingpolicylabel
videooptimizationparameter	Configuration for VideoOptimization parameter

videooptimizationdetectionaction

Configuration for videooptimization detectionaction resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the video optimization detection action. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space ( ), at (@), equals (=), colon (:), and underscore characters.
type	<String>	Read-write	Type of video optimization action. Available settings function as follows:

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			* clear_text_pd - Cleartext PD type is detected. * clear_text_abr - Cleartext ABR is detected. * encrypted_abr - Encrypted ABR is detected. * trigger_enc_abr - Possible encrypted ABR is detected. * trigger_body_detection - Possible cleartext ABR is detected. Triggers body content detection. Possible values = clear_text_pd, clear_text_abr, encrypted_abr, trigger_enc_abr, trigger_body_detection
comment	<String>	Read-write	Comment. Any type of information about this video optimization detection action.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
newname	<String>	Read-write	New name for the videooptimization detection action. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Minimum length = 1
hits	<Integer>	Read-only	The number of times the action has been taken.
referencecount	<Integer>	Read-only	The number of references to the action.
undefhits	<Integer>	Read-only	The number of times the action resulted in UNDEF.
builtin	<String[]>	Read-only	Flag to determine whether video optimization detection action is built-in or not. Possible values = MODIFIABLE, DELETABLE,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			IMMUTABLE, PARTITION_ALL
feature	<String>	Read-only	The feature to be checked while applying this config.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET (ALL)
- GET
- COUNT
- UPDATE
- UNSET
- RENAME

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of

creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/videooptimizationdetectionaction **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"videooptimizationdetectionaction":{

<b>"name":<String_value>,

</b><b>"type":<String_value>,

</b>"comment":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/videooptimizationdetectionaction/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/videooptimizationdetectionaction **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"videooptimizationdetectionaction":{

<b>"name":<String_value>,

</b>"type":<String_value>,

"comment":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/videooptimizationdetectionaction?**action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"videooptimizationdetectionaction":{

<b>"name":<String_value>,

</b>"comment":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

RENAME

URL: http:// <netscaler-ip-address> /nitro/v1/config/videooptimizationdetectionaction?**action=rename HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"videooptimizationdetectionaction":{

<b>"name":<String_value>,

</b><b>"newname":<String_value>
```

```
</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/videooptimizationdetectionaction **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/videooptimizationdetectionaction?**attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/videooptimizationdetectionaction?**filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of videooptimizationdetectionaction resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/videooptimizationdetectionaction?**view=summary**

Use this query-parameter to get the summary output of videooptimizationdetectionaction resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/videooptimizationdetectionaction?**pagesize=#no;pageno=#no**

Use this query-parameter to get the videooptimizationdetectionaction resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "videooptimizationdetectionaction": [ {

"name":<String_value>,

"type":<String_value>,

"hits":<Integer_value>,

"referencecount":<Integer_value>,

"undefhits":<Integer_value>,

"comment":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/videooptimizationdetectionaction/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/ videooptimizationdetectionaction/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/videooptimizationdetectionaction/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of videooptimizationdetectionaction resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "videooptimizationdetectionaction": [ {

"name":<String_value>,

"type":<String_value>,

"hits":<Integer_value>,

"referencecount":<Integer_value>,

"undefhits":<Integer_value>,

"comment":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"_nextgenapiresource":<String_value>
```

```
}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/videooptimizationdetectionaction? **count=yes**
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "videooptimizationdetectionaction": [ { "__count": "#no"} ] }
```

videooptimizationdetectionpolicy

Configuration for videooptimization detectionpolicy resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the videooptimization detection policy. Must begin with a letter, number, or the underscore character

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			(_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters.Can be modified, removed or renamed.
rule	<String>	Read-write	Expression that determines which request or response match the video optimization detection policy. The following requirements apply only to the Citrix ADC CLI: * If the expression includes one or more spaces, enclose the entire expression in double quotation marks. * If the expression itself includes double quotation marks, escape the quotations by using the \ character.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			* Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks.
action	<String>	Read-write	Name of the videooptimization detection action to perform if the request matches this videooptimization detection policy. Built-in actions should be used. These are: * DETECT_CLEARTEXT_PD - Cleartext PD is detected and increment related counters. * DETECT_CLEARTEXT_ABR - Cleartext ABR is detected and increment related counters. * DETECT_ENCRYPTED_ABR - Encrypted ABR is

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			detected and increment related counters. * TRIGGER_ENC_ABR_DETECTION - This is potentially encrypted ABR. Internal traffic heuristics algorithms will further process traffic to confirm detection. * TRIGGER_CT_ABR_BODY_DETECTION - This is potentially cleartext ABR. Internal traffic heuristics algorithms will further process traffic to confirm detection. * RESET - Reset the client connection by closing it. * DROP - Drop the connection without sending a response.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
undefaction	<String>	Read-write	Action to perform if the result of policy evaluation is undefined (UNDEF). An UNDEF event indicates an internal error condition. Only the above built-in actions can be used.
comment	<String>	Read-write	Any type of information about this videooptimization detection policy.
logaction	<String>	Read-write	Name of the messagelog action to use for requests that match this policy.
newname	<String>	Read-write	New name for the videooptimization detection policy. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Minimum length = 1
hits	<Integer>	Read-only	Number of hits.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
undefhits	<Integer>	Read-only	Number of policy UNDEF hits.
builtin	<String[]>	Read-only	Flag to determine if videooptimization detection policy is built-in or not. Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL
feature	<String>	Read-only	The feature to be checked while applying this config.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT
- RENAME

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/videooptimizationdetectionpolicy **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"videooptimizationdetectionpolicy":{

<b>"name":<String_value>,

</b><b>"rule":<String_value>,
```

```
</b><b>"action":<String_value>,

</b>"undefaction":<String_value>,

"comment":<String_value>,

"logaction":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/videooptimizationdetectionpolicy/name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/videooptimizationdetectionpolicy **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"videooptimizationdetectionpolicy":{

<b>"name":<String_value>,

</b>"rule":<String_value>,

"action":<String_value>,

"undefaction":<String_value>,

"comment":<String_value>,

"logaction":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/videooptimizationdetectionpolicy?**action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"videooptimizationdetectionpolicy":{

<b>"name":<String_value>,

</b>"undefaction":true,

"comment":true,

"logaction":true
```

```
}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

RENAME

URL: http:// <netscaler-ip-address> /nitro/v1/config/videooptimizationdetectionpolicy? **action=rename HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"videooptimizationdetectionpolicy":{

<b>"name":<String_value>,

</b><b>"newname":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/videooptimizationdetectionpolicy **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/videooptimizationdetectionpolicy? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/videooptimizationdetectionpolicy?**filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of videooptimizationdetectionpolicy resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/videooptimizationdetectionpolicy?**view=summary**

Use this query-parameter to get the summary output of videooptimizationdetectionpolicy resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/videooptimizationdetectionpolicy?**pagesize=#no;pageno=#no**

Use this query-parameter to get the videooptimizationdetectionpolicy resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "videooptimizationdetectionpolicy": [ {

"name":<String_value>,

"rule":<String_value>,

"action":<String_value>,
```

```
"undefaction":<String_value>,

"hits":<Integer_value>,

"undefhits":<Integer_value>,

"comment":<String_value>,

"logaction":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/videooptimizationdetectionpolicy/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/ videooptimizationdetectionpolicy/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/videooptimizationdetectionpolicy/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of videooptimizationdetectionpolicy resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "videooptimizationdetectionpolicy": [ {

"name":<String_value>,

"rule":<String_value>,

"action":<String_value>,

"undefaction":<String_value>,

"hits":<Integer_value>,

"undefhits":<Integer_value>,

"comment":<String_value>,

"logaction":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/videooptimizationdetectionpolicy? **count=yes**
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "videooptimizationdetectionpolicy": [ { "__count": "#no"} ] }
```

videooptimizationdetectionpolicy_binding

Binding object which returns the resources bound to videooptimizationdetectionpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the videooptimization detection policy for which to display settings.Must provide policy name.
videooptimizationdetectionpolicy_videooptimizationglobaldetection_binding	<videooptimizationdetectionpolicy_videooptimizationglobaldetection_binding[]>	Read-only	videooptimizationglobaldetection that can be bound to videooptimizationdetectionpolicy.
videooptimizationdetectionpolicy_lbvserver_binding	<videooptimizationdetectionpolicy_lbvserver_binding[]>	Read-only	lbvserver that can be bound to videooptimizationdetectionpolicy.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/videooptimizationdetectionpolicy_binding/name_value<String>

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "videooptimizationdetectionpolicy_binding": [ {

"name":<String_value>,

"videooptimizationdetectionpolicy_lbvserver_binding":<videooptimizationdet
ectionpolicy_lbvserver_binding[]_value>,

"videooptimizationdetectionpolicy_videooptimizationglobaldetection_binding
":<videooptimizationdetectionpolicy_videooptimizationglobaldetection_bindi
ng[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/videooptimizationdetectionpolicy_binding

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters:

bulkbindings

http:// <netscaler-ip-address> /nitro/v1/config/videooptimizationdetectionpolicy_binding?**bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "videooptimizationdetectionpolicy_binding": [ {

"name":<String_value>,

"videooptimizationdetectionpolicy_lbvserver_binding":<videooptimizationdet
ectionpolicy_lbvserver_binding[]_value>,

"videooptimizationdetectionpolicy_videooptimizationglobaldetection_binding
":<videooptimizationdetectionpolicy_videooptimizationglobaldetection_bindi
ng[]_value>

}]}
```

videooptimizationdetectionpolicy_lbvserver_binding

Binding object showing the lbvserver that can be bound to videooptimizationdetectionpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
boundto	<String>	Read-write	Location where policy is bound.
name	<String>	Read-write	Name of the videooptimization detection policy for which to display settings.Must provide policy name.
labeltype	<String>	Read-only	Type of policy label invocation. Possible values = vserver, policylabel
priority	<Integer>	Read-only	Specifies the priority of the policy.
activepolicy	<Integer>	Read-only	Indicates whether policy is bound or not.
labelname	<String>	Read-only	Name of the label to invoke if the current policy rule evaluates to TRUE.
gotopriorityexpression	<String>	Read-only	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/ videooptimizationdetectionpolicy_lbvserver_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ videooptimizationdetectionpolicy_lbvserver_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of videooptimizationdetectionpolicy_lbvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ videooptimizationdetectionpolicy_lbvserver_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the videooptimizationdetectionpolicy_lbvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "videooptimizationdetectionpolicy_lbvserver_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"activepolicy":<Integer_value>,

"labelname":<String_value>,

"gotopriorityexpression":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/ videooptimizationdetectionpolicy_lbvserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ videooptimizationdetectionpolicy_lbvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "videooptimizationdetectionpolicy_lbvserver_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"activepolicy":<Integer_value>,

"labelname":<String_value>,
```

```
"gotopriorityexpression":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/ videooptimizationdetectionpolicy_lbvserver_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"videooptimizationdetectionpolicy_lbvserver_binding": [ { "__count":
"#no"} ] }
```

videooptimizationdetectionpolicy_videooptimizationglobaldetection_binding

Binding object showing the videooptimizationglobaldetection that can be bound to videooptimizationdetectionpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the videooptimization detection policy for which to display settings.Must provide policy name.
boundto	<String>	Read-write	Location where policy is bound.
activepolicy	<Integer>	Read-only	Indicates whether policy is bound or not.
priority	<Integer>	Read-only	Specifies the priority of the policy.
labeltype	<String>	Read-only	Type of policy label invocation. Possible values = vserver, policylabel
gotopriorityexpression	<String>	Read-only	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
labelname	<String>	Read-only	Name of the label to invoke if the current policy rule evaluates to TRUE.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/ videooptimizationdetectionpolicy_videooptimizationglobaldetection_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ videooptimizationdetectionpolicy_videooptimizationglobaldetection_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of videooptimizationdetectionpolicy_videooptimizationglobaldetection_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ videooptimizationdetectionpolicy_videooptimizationglobaldetection_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the videooptimizationdetectionpolicy_videooptimizationglobaldetection_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "videooptimizationdetectionpolicy_videooptimizationglobaldetection_bind
ing": [ {

"name":<String_value>,

"boundto":<String_value>,

"activepolicy":<Integer_value>,

"priority":<Integer_value>,

"labeltype":<String_value>,

"gotopriorityexpression":<String_value>,

"labelname":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/ videooptimizationdetectionpolicy_videooptimizationglobaldetection_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ videooptimizationdetectionpolicy_videooptimizationglobaldetection_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "videooptimizationdetectionpolicy_videooptimizationglobaldetection_bind
ing": [ {

"name":<String_value>,

"boundto":<String_value>,

"activepolicy":<Integer_value>,

"priority":<Integer_value>,

"labeltype":<String_value>,

"gotopriorityexpression":<String_value>,
```

```
"labelname":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/ videooptimizationdetectionpolicy_videooptimizationglobaldetection_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"videooptimizationdetectionpolicy_videooptimizationglobaldetection_bindin
g": [ { "__count": "#no"} ] }
```

videooptimizationdetectionpolicylabel

Configuration for videooptimization detection policy label resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
labelname	<String>	Read-write	Name for the Video optimization

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			detection policy label. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after the videooptimization detection policy label is added. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my videooptimization detection policy label" or my videooptimization

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			detection policy label').
policylabeltype	<String>	Read-write	Type of responses sent by the policies bound to this policy label. Types are: * HTTP - HTTP responses. * OTHERTCP - NON-HTTP TCP responses. Default value: NS_PLTMAP_RSP_REQ Possible values = videoopt_req, videoopt_res
comment	<String>	Read-write	Any comments to preserve information about this videooptimization detection policy label.
newname	<String>	Read-write	New name for the videooptimization detection policy label. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			-), period (.) hash (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Minimum length = 1
numpol	<Integer>	Read-only	number of polices bound to label.
hits	<Integer>	Read-only	Number of times policy label was invoked.
priority	<Integer>	Read-only	Specifies the priority of the policy.
gotopriorityexpression	<String>	Read-only	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
labeltype	<String>	Read-only	Type of policy label to invoke. Available settings function as follows: * vserver - Invoke an unnamed policy label associated with a virtual server. * policylabel - Invoke a user-defined policy label.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = vserver, policylabel
invoke_labelname	<String>	Read-only	* If labelType is policylabel, name of the policy label to invoke. * If labelType is reqvserver or resvserver, name of the virtual server.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET (ALL)
- GET
- COUNT
- RENAME

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/videooptimizationdetectionpolicylabel **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"videooptimizationdetectionpolicylabel":{

<b>"labelname":<String_value>,

</b>"policylabeltype":<String_value>,

"comment":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/videooptimizationdetectionpolicylabel/labelname_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

RENAME

URL: http:// <netscaler-ip-address> /nitro/v1/config/videooptimizationdetectionpolicylabel?**action=rename HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"videooptimizationdetectionpolicylabel":{

<b>"labelname":<String_value>,

</b><b>"newname":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/videooptimizationdetectionpolicylabel **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/videooptimizationdetectionpolicylabel? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/videooptimizationdetectionpolicylabel? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of videooptimizationdetectionpolicylabel resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/videooptimizationdetectionpolicylabel? **view=summary**

Use this query-parameter to get the summary output of videooptimizationdetectionpolicylabel resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/videooptimizationdetectionpolicylabel? **pagesize=#no;pageno=#no**

Use this query-parameter to get the videooptimizationdetectionpolicylabel resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "videooptimizationdetectionpolicylabel": [ {

"labelname":<String_value>,

"policylabeltype":<String_value>,

"numpol":<Integer_value>,

"hits":<Integer_value>,

"priority":<Integer_value>,

"gotopriorityexpression":<String_value>,

"labeltype":<String_value>,

"invoke_labelname":<String_value>,

"comment":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/videooptimizationdetectionpolicylabel/ labelname_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/ videooptimizationdetectionpolicylabel/ labelname_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/videooptimizationdetectionpolicylabel/ labelname_value<String> ? **view=summary**

Use this query-parameter to get the summary output of videooptimizationdetectionpolicylabel resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "videooptimizationdetectionpolicylabel": [ {

"labelname":<String_value>,

"policylabeltype":<String_value>,

"numpol":<Integer_value>,

"hits":<Integer_value>,

"priority":<Integer_value>,

"gotopriorityexpression":<String_value>,

"labeltype":<String_value>,

"invoke_labelname":<String_value>,

"comment":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/videooptimizationdetectionpolicylabel?**count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "videooptimizationdetectionpolicylabel": [ { "__count": "#no"} ] }
```

videooptimizationdetectionpolicylabel_binding

Binding object which returns the resources bound to videooptimizationdetectionpolicylabel.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
labelname	<String>	Read-write	Name of the videooptimization detection policy label.
videooptimizationdetectionpolicylabel_videooptimizationdetectionpolicy_binding	<videooptimizationdetectionpolicylabel_videooptimizationdetectionpolicy_binding[]>	Read-only	videooptimizationdetectionpolicy that can be bound to videooptimizationdetectionpolicylabel.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
videooptimizationdetectionpolicylabel_policybinding_binding	<videooptimizationdetectionpolicylabel_policybinding_binding[]>	Read-only	policybinding that can be bound to videooptimizationdetectionpolicylabel.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/videooptimizationdetectionpolicylabel_binding/labelname_value<String>

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "videooptimizationdetectionpolicylabel_binding": [ {

"labelname":<String_value>,

"videooptimizationdetectionpolicylabel_policybinding_binding":<videooptimi
zationdetectionpolicylabel_policybinding_binding[]_value>,

"videooptimizationdetectionpolicylabel_videooptimizationdetectionpolicy_bi
nding":<videooptimizationdetectionpolicylabel_videooptimizationdetectionpo
licy_binding[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/videooptimizationdetectionpolicylabel_binding

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters:

bulkbindings

http:// <netscaler-ip-address> /nitro/v1/config/videooptimizationdetectionpolicylabel_binding?**bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "videooptimizationdetectionpolicylabel_binding": [ {

"labelname":<String_value>,

"videooptimizationdetectionpolicylabel_policybinding_binding":<videooptimi
zationdetectionpolicylabel_policybinding_binding[]_value>,

"videooptimizationdetectionpolicylabel_videooptimizationdetectionpolicy_bi
nding":<videooptimizationdetectionpolicylabel_videooptimizationdetectionpo
licy_binding[]_value>

}]}
```

videooptimizationdetectionpolicylabel_policybinding_binding

Binding object showing the policybinding that can be bound to videooptimizationdetectionpolicylabel.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
invoke_labelname	<String>	Read-write	* If labelType is policylabel, name of the policy label to invoke. * If labelType is reqvserver or resvserver, name of the virtual server.
invoke	<Boolean>	Read-write	If the current policy evaluates to TRUE, terminate evaluation of policies bound to the current policy label and evaluate the specified policy label.
gotopriorityexpression	<String>	Read-write	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
policyname	<String>	Read-write	Name of the videooptimization policy.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
priority	<Integer>	Read-write	Specifies the priority of the policy.
labeltype	<String>	Read-write	Type of policy label to invoke. Available settings function as follows: * vserver - Invoke an unnamed policy label associated with a virtual server. * policylabel - Invoke a user-defined policy label. Possible values = vserver, policylabel
labelname	<String>	Read-write	Name of the videooptimization detection policy label to which to bind the policy.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/ videooptimizationdetectionpolicylabel_policybinding_binding/ labelname_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ videooptimizationdetectionpolicylabel_policybinding_binding/ labelname_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of videooptimizationdetectionpolicylabel_policybinding_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ videooptimizationdetectionpolicylabel_policybinding_binding/ labelname_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the videooptimizationdetectionpolicylabel_policybinding_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "videooptimizationdetectionpolicylabel_policybinding_binding": [ {

"invoke_labelname":<String_value>,

"invoke":<Boolean_value>,

"gotopriorityexpression":<String_value>,

"policyname":<String_value>,

"priority":<Integer_value>,

"labeltype":<String_value>,

"labelname":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/ videooptimizationdetectionpolicylabel_policybinding_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ videooptimizationdetectionpolicylabel_policybinding_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "videooptimizationdetectionpolicylabel_policybinding_binding": [ {

"invoke_labelname":<String_value>,

"invoke":<Boolean_value>,

"gotopriorityexpression":<String_value>,

"policyname":<String_value>,

"priority":<Integer_value>,

"labeltype":<String_value>,

"labelname":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/ videooptimizationdetectionpolicylabel_policybinding_binding/ labelname_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"videooptimizationdetectionpolicylabel_policybinding_binding":
[ { "__count": "#no"} ] }
```

videooptimizationdetectionpolicylabel_videooptimizationdetectionpolicy_binding

Binding object showing the videooptimizationdetectionpolicy that can be bound to videooptimizationdetectionpolicylabel.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
labeltype	<String>	Read-write	Type of policy label to invoke. Available settings function as follows: * vserver - Invoke an unnamed policy label associated with a virtual server. * policylabel - Invoke a user-defined policy label. Possible values = vserver, policylabel

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
priority	<Integer>	Read-write	Specifies the priority of the policy.
labelname	<String>	Read-write	Name of the videooptimization detection policy label to which to bind the policy.
invoke_labelname	<String>	Read-write	* If labelType is policylabel, name of the policy label to invoke. * If labelType is reqvserver or resvserver, name of the virtual server.
policyname	<String>	Read-write	Name of the videooptimization policy.
gotopriorityexpression	<String>	Read-write	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
invoke	<Boolean>	Read-write	If the current policy evaluates to TRUE, terminate evaluation of policies bound to the current policy label and evaluate the specified policy label.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/ videooptimizationdetectionpolicylabel_videooptimizationdetectionpolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"videooptimizationdetectionpolicylabel_videooptimizationdetectionpolicy_bi
nding":{

<b>"labelname":<String_value>,

</b><b>"policyname":<String_value>,

</b><b>"priority":<Integer_value>,

</b>"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>,

"labeltype":<String_value>,

"invoke_labelname":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/ videooptimizationdetectionpolicylabel_videooptimizationdetectionpolicy_binding/ labelname_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ videooptimizationdetectionpolicylabel_videooptimizationdetectionpolicy_binding/ labelname_value<String> ? **args= policyname:<String_value>, priority: <Integer_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/ videooptimizationdetectionpolicylabel_videooptimizationdetectionpolicy_binding/ labelname_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ videooptimizationdetectionpolicylabel_videooptimizationdetectionpolicy_binding/ labelname_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of videooptimizationdetectionpolicylabel_videooptimizationdetectionpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ videooptimizationdetectionpolicylabel_videooptimizationdetectionpolicy_binding/ labelname_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the videooptimizationdetectionpolicylabel_videooptimizationdetectionpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "videooptimizationdetectionpolicylabel_videooptimizationdetectionpolicy
_binding": [ {

"labeltype":<String_value>,

"priority":<Integer_value>,

"labelname":<String_value>,

"invoke_labelname":<String_value>,

"policyname":<String_value>,

"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/ videooptimizationdetectionpolicylabel_videooptimizationdetectionpolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ videooptimizationdetectionpolicylabel_videooptimizationdetectionpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "videooptimizationdetectionpolicylabel_videooptimizationdetectionpolicy
_binding": [ {

"labeltype":<String_value>,

"priority":<Integer_value>,

"labelname":<String_value>,

"invoke_labelname":<String_value>,

"policyname":<String_value>,

"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/ videooptimizationdetectionpolicylabel_videooptimizationdetectionpolicy_binding/ labelname_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"videooptimizationdetectionpolicylabel_videooptimizationdetectionpolicy_binding": [ { "__count": "#no"} ] }
```

videooptimizationglobaldetection_binding

Binding object which returns the resources bound to videooptimizationglobaldetection.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
videooptimizationglobaldetection_videooptimizationdetectionpolicy_binding	<videooptimizationglobaldetection_videooptimizationdetectionpolicy_binding[]>	Read-write	videooptimizationdetectionpolicy that can be bound to videooptimizationglobaldetection.

Operations

(click to see Properties)

- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/videooptimizationglobaldetection_binding

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "videooptimizationglobaldetection_binding": [ {

"videooptimizationglobaldetection_videooptimizationdetectionpolicy_binding
```

```
":<videooptimizationglobaldetection_videooptimizationdetectionpolicy_binding[]_value>

}]}
```

videooptimizationglobaldetection_videooptimizationdetectionpolicy_binding

Binding object showing the videooptimizationdetectionpolicy that can be bound to videooptimizationglobaldetection.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
gotopriorityexpression	<String>	Read-write	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
invoke	<Boolean>	Read-write	If the current policy evaluates to TRUE, terminate evaluation of policies bound to the current policy label, and then forward the request to the specified virtual server or evaluate the specified policy label.
policyname	<String>	Read-write	Name of the videooptimization detection policy.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
globalbindtype	<String>	Read-write	. Default value: SYSTEM_GLOBAL Possible values = SYSTEM_GLOBAL, VPN_GLOBAL, RNAT_GLOBAL, APPFW_GLOBAL, TM_GLOBAL
type	<String>	Read-write	Specifies the bind point whose policies you want to display. Possible values = REQ_OVERRIDE, REQ_DEFAULT, RES_OVERRIDE, RES_DEFAULT
labelname	<String>	Read-write	Name of the policy label to invoke. If the current policy evaluates to TRUE, the invoke parameter is set, and Label Type is policylabel.
labeltype	<String>	Read-write	Type of invocation, Available settings function as follows: * vserver - Forward the request to the specified virtual server. * policylabel - Invoke the specified policy label. Possible values = vserver, policylabel

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
priority	<Integer>	Read-write	Specifies the priority of the policy.
numpol	<Integer>	Read-only	number of polices bound.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/ videooptimizationglobaldetection_videooptimizationdetectionpolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"videooptimizationglobaldetection_videooptimizationdetectionpolicy_binding
":{

<b>"policyname":<String_value>,

</b><b>"priority":<Integer_value>,

</b>"gotopriorityexpression":<String_value>,

"type":<String_value>,

"invoke":<Boolean_value>,

"labeltype":<String_value>,

"labelname":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/ videooptimizationglobaldetection_videooptimizationdetectionpolicy_binding **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ videooptimizationglobaldetection_videooptimizationdetectionpolicy_binding? **args= policyname:<String_value>, type: <String_value> ,priority: <Integer_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/ videooptimizationglobaldetection_videooptimizationdetectionpolicy_binding **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ videooptimizationglobaldetection_videooptimizationdetectionpolicy_binding? **args=type: <String_value>**

Use this query-parameter to get videooptimizationglobaldetection_videooptimizationdetectionpolicy_binding resources based on additional properties.

filter http:// <netscaler-ip-address> /nitro/v1/config/ videooptimizationglobaldetection_videooptimizationdetectionpolicy_binding? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of videooptimizationglobaldetection_videooptimizationdetectionpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ videooptimizationglobaldetection_videooptimizationdetectionpolicy_binding? **pagesize=#no;pageno=#no**

Use this query-parameter to get the videooptimizationglobaldetection_videooptimizationdetectionpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "videooptimizationglobaldetection_videooptimizationdetectionpolicy_bind
ing": [ {

"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>,

"policyname":<String_value>,

"globalbindtype":<String_value>,

"type":<String_value>,

"labelname":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"numpol":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/ videooptimizationglobaldetection_videooptimizationdetectionpolicy_binding? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "videooptimizationglobaldetection_videooptimizationdetectionpolicy_binding": [ { "__count": "#no"} ] }
```

videooptimizationglobalpacing_binding

Binding object which returns the resources bound to videooptimizationglobalpacing.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
videooptimizationglobalpacing_videooptimizationpacingpolicy_binding	<videooptimizationglobalpacing_videooptimizationpacingpolicy_binding[]>	Read-write	videooptimizationpacingpolicy that can be bound to videooptimizationglobalpacing.

Operations

(click to see Properties)

- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/videooptimizationglobalpacing_binding

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "videooptimizationglobalpacing_binding": [ {

"videooptimizationglobalpacing_videooptimizationpacingpolicy_binding":<videooptimizationglobalpacing_videooptimizationpacingpolicy_binding[]_value>

}]}
```

videooptimizationglobalpacing_videooptimizationpacingpolicy_binding

Binding object showing the videooptimizationpacingpolicy that can be bound to videooptimizationglobalpacing.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
type	<String>	Read-write	Specifies the bind point whose policies you want to display. Possible values = REQ_OVERRIDE, REQ_DEFAULT, RES_OVERRIDE, RES_DEFAULT

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
invoke	<Boolean>	Read-write	If the current policy evaluates to TRUE, terminate evaluation of policies bound to the current policy label, and then forward the request to the specified virtual server or evaluate the specified policy label.
gotopriorityexpression	<String>	Read-write	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
policyname	<String>	Read-write	Name of the videooptimization pacing policy.
globalbindtype	<String>	Read-write	. Default value: SYSTEM_GLOBAL Possible values = SYSTEM_GLOBAL, VPN_GLOBAL, RNAT_GLOBAL, APPFW_GLOBAL, TM_GLOBAL
priority	<Integer>	Read-write	Specifies the priority of the policy.
labeltype	<String>	Read-write	Type of invocation, Available settings

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			function as follows: * vserver - Forward the request to the specified virtual server. * policylabel - Invoke the specified policy label. Possible values = vserver, policylabel
labelname	<String>	Read-write	Name of the policy label to invoke. If the current policy evaluates to TRUE, the invoke parameter is set, and Label Type is policylabel.
numpol	<Integer>	Read-only	number of polices bound.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/ videooptimizationglobalpacing_videooptimizationpacingpolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"videooptimizationglobalpacing_videooptimizationpacingpolicy_binding":{

<b>"policyname":<String_value>,

</b><b>"priority":<Integer_value>,

</b>"gotopriorityexpression":<String_value>,

"type":<String_value>,
```

```
"invoke":<Boolean_value>,

"labeltype":<String_value>,

"labelname":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/ videooptimizationglobalpacing_videooptimizationpacingpolicy_binding **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ videooptimizationglobalpacing_videooptimizationpacingpolicy_binding? **args= policyname:<String_value>, type: <String_value> ,priority: <Integer_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/ videooptimizationglobalpacing_videooptimizationpacingpolicy_binding **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ videooptimizationglobalpacing_videooptimizationpacingpolicy_binding? **args=type: <String_value>**

Use this query-parameter to get videooptimizationglobalpacing_videooptimizationpacingpolicy_binding resources based on additional properties.

filter http:// <netscaler-ip-address> /nitro/v1/config/ videooptimizationglobalpacing_videooptimizationpacingpolicy_binding? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of videooptimizationglobalpacing_videooptimizationpacingpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ videooptimizationglobalpacing_videooptimizationpacingpolicy_binding? **pagesize=#no;pageno=#no**

Use this query-parameter to get the videooptimizationglobalpacing_videooptimizationpacingpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "videooptimizationglobalpacing_videooptimizationpacingpolicy_binding":
[ {

"type":<String_value>,

"invoke":<Boolean_value>,
```

```
"gotopriorityexpression":<String_value>,

"policyname":<String_value>,

"globalbindtype":<String_value>,

"priority":<Integer_value>,

"labeltype":<String_value>,

"labelname":<String_value>,

"numpol":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/ videooptimizationglobalpacing_videooptimizationpacingpolicy_binding? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "videooptimizationglobalpacing_videooptimizationpacingpolicy_binding":
[ { "__count": "#no"} ] }
```

videooptimizationpacingaction

Configuration for videooptimization pacingaction resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the video optimization pacing action. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space ( ), at (@), equals (=), colon (:), and underscore characters.
rate	<Integer>	Read-write	ABR Video Optimization Pacing Rate (in Kbps). Default value: 1000 Minimum value = 1 Maximum value = 2147483647
comment	<String>	Read-write	Comment. Any type of information about this video optimization detection action.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
newname	<String>	Read-write	New name for the videooptimization pacing action. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Minimum length = 1
hits	<Integer>	Read-only	The number of times the action has been taken.
referencecount	<Integer>	Read-only	The number of references to the action.
undefhits	<Integer>	Read-only	The number of times the action resulted in UNDEF.
builtin	<String[]>	Read-only	Flag to determine whether video optimization detection action is built-in or not. Possible values = MODIFIABLE, DELETABLE,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			IMMUTABLE, PARTITION_ALL
feature	<String>	Read-only	The feature to be checked while applying this config.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET (ALL)
- GET
- COUNT
- UPDATE
- UNSET
- RENAME

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of

creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/videooptimizationpacingaction **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"videooptimizationpacingaction":{

<b>"name":<String_value>,

</b><b>"rate":<Integer_value>,

</b>"comment":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/videooptimizationpacingaction/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/videooptimizationpacingaction **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"videooptimizationpacingaction":{

<b>"name":<String_value>,

</b>"rate":<Integer_value>,

"comment":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/videooptimizationpacingaction? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"videooptimizationpacingaction":{

<b>"name":<String_value>,

</b>"rate":true,

"comment":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

RENAME

URL: http:// <netscaler-ip-address> /nitro/v1/config/videooptimizationpacingaction? **action=rename HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"videooptimizationpacingaction":{

<b>"name":<String_value>,
```

```
</b><b>"newname":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/videooptimizationpacingaction **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/videooptimizationpacingaction? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/videooptimizationpacingaction? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of videooptimizationpacingaction resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/videooptimizationpacingaction? **view=summary**

Use this query-parameter to get the summary output of videooptimizationpacingaction resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/videooptimizationpacingaction? **pagesize=#no;pageno=#no**

Use this query-parameter to get the videooptimizationpacingaction resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "videooptimizationpacingaction": [ {

"name":<String_value>,

"hits":<Integer_value>,

"referencecount":<Integer_value>,

"undefhits":<Integer_value>,

"rate":<Integer_value>,

"comment":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/videooptimizationpacingaction/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/ videooptimizationpacingaction/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/videooptimizationpacingaction/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of videooptimizationpacingaction resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "videooptimizationpacingaction": [ {

"name":<String_value>,

"hits":<Integer_value>,

"referencecount":<Integer_value>,

"undefhits":<Integer_value>,

"rate":<Integer_value>,

"comment":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"_nextgenapiresource":<String_value>
```

```
}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/videooptimizationpacingaction? **count=yes**
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "videooptimizationpacingaction": [ { "__count": "#no"} ] }
```

videooptimizationpacingpolicy

Configuration for videooptimization pacingpolicy resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the videooptimization pacing policy. Must begin with a letter, number, or the underscore character

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			(_), and must contain only letters, numbers, and the hyphen (-), period (.) pound (#), space ( ), at (@), equals (=), colon (:), and underscore characters.Can be modified, removed or renamed.
rule	<String>	Read-write	Expression that determines which request or response match the video optimization pacing policy. The following requirements apply only to the Citrix ADC CLI: * If the expression includes one or more spaces, enclose the entire expression in double quotation marks. * If the expression itself includes double quotation marks, escape the quotations by using the \ character.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			* Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks.
action	<String>	Read-write	Name of the videooptimization pacing action to perform if the request matches this videooptimization pacing policy.
undefaction	<String>	Read-write	Action to perform if the result of policy evaluation is undefined (UNDEF). An UNDEF event indicates an internal error condition. Only the above built-in actions can be used.
comment	<String>	Read-write	Any type of information about this videooptimization pacing policy.
logaction	<String>	Read-write	Name of the messagelog action to use for requests that match this policy.
newname	<String>	Read-write	New name for the videooptimization

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			pacing policy. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Minimum length = 1
hits	<Integer>	Read-only	Number of hits.
undefhits	<Integer>	Read-only	Number of policy UNDEF hits.
builtin	<String[]>	Read-only	Flag to determine if videooptimization pacing policy is built-in or not. Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL
feature	<String>	Read-only	The feature to be checked while applying this config.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT
- RENAME

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/videooptimizationpacingpolicy **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"videooptimizationpacingpolicy":{

<b>"name":<String_value>,

</b><b>"rule":<String_value>,

</b><b>"action":<String_value>,

</b>"undefaction":<String_value>,

"comment":<String_value>,

"logaction":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/videooptimizationpacingpolicy/name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/videooptimizationpacingpolicy **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"videooptimizationpacingpolicy":{

<b>"name":<String_value>,

</b>"rule":<String_value>,

"action":<String_value>,

"undefaction":<String_value>,

"comment":<String_value>,

"logaction":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/videooptimizationpacingpolicy? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"videooptimizationpacingpolicy":{

<b>"name":<String_value>,

</b>"undefaction":true,

"comment":true,

"logaction":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

RENAME

URL: http:// <netscaler-ip-address> /nitro/v1/config/videooptimizationpacingpolicy?**action=rename HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"videooptimizationpacingpolicy":{

<b>"name":<String_value>,

</b><b>"newname":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/videooptimizationpacingpolicy **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/videooptimizationpacingpolicy? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/videooptimizationpacingpolicy? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of videooptimizationpacingpolicy resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/videooptimizationpacingpolicy? **view=summary**

Use this query-parameter to get the summary output of videooptimizationpacingpolicy resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/videooptimizationpacingpolicy? **pagesize=#no;pageno=#no**

Use this query-parameter to get the videooptimizationpacingpolicy resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "videooptimizationpacingpolicy": [ {

"name":<String_value>,

"rule":<String_value>,

"action":<String_value>,

"undefaction":<String_value>,

"hits":<Integer_value>,

"undefhits":<Integer_value>,

"comment":<String_value>,

"logaction":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/videooptimizationpacingpolicy/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/ videooptimizationpacingpolicy/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/videooptimizationpacingpolicy/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of videooptimizationpacingpolicy resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "videooptimizationpacingpolicy": [ {

"name":<String_value>,

"rule":<String_value>,

"action":<String_value>,

"undefaction":<String_value>,

"hits":<Integer_value>,

"undefhits":<Integer_value>,

"comment":<String_value>,

"logaction":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"_nextgenapiresource":<String_value>
```

```
}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/videooptimizationpacingpolicy? **count=yes**
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "videooptimizationpacingpolicy": [ { "__count": "#no"} ] }
```

videooptimizationpacingpolicy_binding

Binding object which returns the resources bound to videooptimizationpacingpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the videooptimization pacing policy for which to display settings.Must provide policy name.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
videooptimizationpacingpolicy_lbvserver_binding	<videooptimizationpacingpolicy_lbvserver_binding[]>	Read-only	lbvserver that can be bound to videooptimizationpacingpolicy.
videooptimizationpacingpolicy_videooptimizationglobalpacing_binding	<videooptimizationpacingpolicy_videooptimizationglobalpacing_binding[]>	Read-only	videooptimizationglobalpacing that can be bound to videooptimizationpacingpolicy.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/videooptimizationpacingpolicy_binding/name_value<String>

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "videooptimizationpacingpolicy_binding": [ {

"name":<String_value>,

"videooptimizationpacingpolicy_lbvserver_binding":<videooptimizationpacing
policy_lbvserver_binding[]_value>,

"videooptimizationpacingpolicy_videooptimizationglobalpacing_binding":<vid
eooptimizationpacingpolicy_videooptimizationglobalpacing_binding[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/videooptimizationpacingpolicy_binding

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters:

bulkbindings

http:// <netscaler-ip-address> /nitro/v1/config/videooptimizationpacingpolicy_binding?**bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "videooptimizationpacingpolicy_binding": [ {

"name":<String_value>,

"videooptimizationpacingpolicy_lbvserver_binding":<videooptimizationpacing
policy_lbvserver_binding[]_value>,

"videooptimizationpacingpolicy_videooptimizationglobalpacing_binding":<vid
eooptimizationpacingpolicy_videooptimizationglobalpacing_binding[]_value>
```

```
}]}
```

videooptimizationpacingpolicy_lbvserver_binding

Binding object showing the lbvserver that can be bound to videooptimizationpacingpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the videooptimization pacing policy for which to display settings.Must provide policy name.
boundto	<String>	Read-write	Location where policy is bound.
labeltype	<String>	Read-only	Type of policy label invocation. Possible values = vserver, policylabel
priority	<Integer>	Read-only	Specifies the priority of the policy.
activepolicy	<Integer>	Read-only	Indicates whether policy is bound or not.
labelname	<String>	Read-only	Name of the label to invoke if the current policy rule evaluates to TRUE.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
gotopriorityexpression	<String>	Read-only	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/ videooptimizationpacingpolicy_lbvserver_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/videooptimizationpacingpolicy_lbvserver_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of videooptimizationpacingpolicy_lbvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ videooptimizationpacingpolicy_lbvserver_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the videooptimizationpacingpolicy_lbvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "videooptimizationpacingpolicy_lbvserver_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"activepolicy":<Integer_value>,

"labelname":<String_value>,

"gotopriorityexpression":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/ videooptimizationpacingpolicy_lbvserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ videooptimizationpacingpolicy_lbvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "videooptimizationpacingpolicy_lbvserver_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"activepolicy":<Integer_value>,

"labelname":<String_value>,

"gotopriorityexpression":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/ videooptimizationpacingpolicy_lbvserver_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"videooptimizationpacingpolicy_lbvserver_binding": [ { "__count":
"#no"} ] }
```

videooptimizationpacingpolicy_videooptimizationglobalpacing_binding

Binding object showing the videooptimizationglobalpacing that can be bound to videooptimizationpacingpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
boundto	<String>	Read-write	Location where policy is bound.
name	<String>	Read-write	Name of the videooptimization pacing policy for which to display settings.Must provide policy name.
labeltype	<String>	Read-only	Type of policy label invocation. Possible values = vserver, policylabel
priority	<Integer>	Read-only	Specifies the priority of the policy.
activepolicy	<Integer>	Read-only	Indicates whether policy is bound or not.
labelname	<String>	Read-only	Name of the label to invoke if the current policy rule evaluates to TRUE.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
gotopriorityexpression	<String>	Read-only	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/ videooptimizationpacingpolicy_videooptimizationglobalpacing_binding/ name_value<String>
Query-parameters: filter http:// <netscaler-ip-address> /nitro/v1/config/ videooptimizationpacingpolicy_videooptimizationglobalpacing_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of videooptimizationpacingpolicy_videooptimizationglobalpacing_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ videooptimizationpacingpolicy_videooptimizationglobalpacing_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the videooptimizationpacingpolicy_videooptimizationglobalpacing_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "videooptimizationpacingpolicy_videooptimizationglobalpacing_binding":
[ {

"boundto":<String_value>,

"name":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"activepolicy":<Integer_value>,

"labelname":<String_value>,

"gotopriorityexpression":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/ videooptimizationpacingpolicy_videooptimizationglobalpacing_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ videooptimizationpacingpolicy_videooptimizationglobalpacing_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "videooptimizationpacingpolicy_videooptimizationglobalpacing_binding":
[ {

"boundto":<String_value>,

"name":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"activepolicy":<Integer_value>,

"labelname":<String_value>,

"gotopriorityexpression":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/ videooptimizationpacingpolicy_videooptimizationglobalpacing_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"videooptimizationpacingpolicy_videooptimizationglobalpacing_binding":
[ { "__count": "#no"} ] }
```

videooptimizationpacingpolicylabel

Configuration for videooptimization pacing policy label resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
labelname	<String>	Read-write	Name for the Video optimization pacing policy label. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Cannot be changed after the videooptimization pacing policy label is added. The following requirement applies

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my videooptimization pacing policy label" or my videooptimization pacing policy label').
policylabeltype	<String>	Read-write	Type of responses sent by the policies bound to this policy label. Types are: * HTTP - HTTP responses. * OTHERTCP - NON-HTTP TCP responses. Default value: NS_PLTMAP_RSP_REQ Possible values = videoopt_req, videoopt_res
comment	<String>	Read-write	Any comments to preserve information about this

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			videooptimization pacing policy label.
newname	<String>	Read-write	New name for the videooptimization pacing policy label. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space ( ), at (@), equals (=), colon (:), and underscore characters. Minimum length = 1
numpol	<Integer>	Read-only	number of polices bound to label.
hits	<Integer>	Read-only	Number of times policy label was invoked.
priority	<Integer>	Read-only	Specifies the priority of the policy.
gotopriorityexpression	<String>	Read-only	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
labeltype	<String>	Read-only	Type of policy label to invoke. Available settings function as follows: * vserver - Invoke an unnamed policy label associated with a virtual server. * policylabel - Invoke a user-defined policy label. Possible values = vserver, policylabel
invoke_labelname	<String>	Read-only	* If labelType is policylabel, name of the policy label to invoke. * If labelType is reqvserver or resvserver, name of the virtual server.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET (ALL)
- GET
- COUNT

- RENAME

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/videooptimizationpacingpolicylabel **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"videooptimizationpacingpolicylabel":{

<b>"labelname":<String_value>,

</b>"policylabeltype":<String_value>,

"comment":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/videooptimizationpacingpolicylabel/ labelname_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

RENAME

URL: http:// <netscaler-ip-address> /nitro/v1/config/videooptimizationpacingpolicylabel? **action=rename HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"videooptimizationpacingpolicylabel":{

<b>"labelname":<String_value>,

</b><b>"newname":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/videooptimizationpacingpolicylabel **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/videooptimizationpacingpolicylabel? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/videooptimizationpacingpolicylabel? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of videooptimizationpacingpolicylabel resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/videooptimizationpacingpolicylabel? **view=summary**

Use this query-parameter to get the summary output of videooptimizationpacingpolicylabel resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/videooptimizationpacingpolicylabel? **pagesize=#no;pageno=#no**

Use this query-parameter to get the videooptimizationpacingpolicylabel resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "videooptimizationpacingpolicylabel": [ {

"labelname":<String_value>,

"policylabeltype":<String_value>,

"numpol":<Integer_value>,

"hits":<Integer_value>,

"priority":<Integer_value>,

"gotopriorityexpression":<String_value>,

"labeltype":<String_value>,

"invoke_labelname":<String_value>,

"comment":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/videooptimizationpacingpolicylabel/ labelname_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/ videooptimizationpacingpolicylabel/ labelname_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/videooptimizationpacingpolicylabel/ labelname_value<String> ? **view=summary**

Use this query-parameter to get the summary output of videooptimizationpacingpolicylabel resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "videooptimizationpacingpolicylabel": [ {

"labelname":<String_value>,

"policylabeltype":<String_value>,

"numpol":<Integer_value>,

"hits":<Integer_value>,
```

```
"priority":<Integer_value>,

"gotopriorityexpression":<String_value>,

"labeltype":<String_value>,

"invoke_labelname":<String_value>,

"comment":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/videooptimizationpacingpolicylabel?**count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "videooptimizationpacingpolicylabel": [ { "__count": "#no"} ] }
```

videooptimizationpacingpolicylabel_binding

Binding object which returns the resources bound to videooptimizationpacingpolicylabel.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
labelname	<String>	Read-write	Name of the videooptimization pacing policy label.
videooptimizationpacingpolicylabel_videooptimizationpacingpolicy_binding	<videooptimizationpacingpolicylabel_videooptimizationpacingpolicy_binding[]>	Read-only	videooptimizationpacingpolicy that can be bound to videooptimizationpacingpolicylabel.
videooptimizationpacingpolicylabel_policybinding_binding	<videooptimizationpacingpolicylabel_policybinding_binding[]>	Read-only	policybinding that can be bound to videooptimizationpacingpolicylabel.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.
- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/videooptimizationpacingpolicylabel_binding/labelname_value<String>

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "videooptimizationpacingpolicylabel_binding": [ {

"labelname":<String_value>,

"videooptimizationpacingpolicylabel_policybinding_binding":<videooptimizat
ionpacingpolicylabel_policybinding_binding[]_value>,
```

```
"videooptimizationpacingpolicylabel_videooptimizationpacingpolicy_binding"
:<videooptimizationpacingpolicylabel_videooptimizationpacingpolicy_binding
[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/videooptimizationpacingpolicylabel_binding

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters:

bulkbindings

http:// <netscaler-ip-address> /nitro/v1/config/videooptimizationpacingpolicylabel_binding?**bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "videooptimizationpacingpolicylabel_binding": [ {

"labelname":<String_value>,

"videooptimizationpacingpolicylabel_policybinding_binding":<videooptimizat
ionpacingpolicylabel_policybinding_binding[]_value>,

"videooptimizationpacingpolicylabel_videooptimizationpacingpolicy_binding"
:<videooptimizationpacingpolicylabel_videooptimizationpacingpolicy_binding
[]_value>

}]}
```

videooptimizationpacingpolicylabel_policybinding_binding

Binding object showing the policybinding that can be bound to videooptimizationpacingpolicylabel.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
priority	<Integer>	Read-write	Specifies the priority of the policy.
labeltype	<String>	Read-write	Type of policy label to invoke. Available settings function as follows: * vserver - Invoke an unnamed policy label associated with a virtual server. * policylabel - Invoke a user-defined policy label. Possible values = vserver, policylabel

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
labelname	<String>	Read-write	Name of the videooptimization pacing policy label to which to bind the policy.
policyname	<String>	Read-write	Name of the videooptimization policy.
invoke	<Boolean>	Read-write	If the current policy evaluates to TRUE, terminate evaluation of policies bound to the current policy label and evaluate the specified policy label.
gotopriorityexpression	<String>	Read-write	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
invoke_labelname	<String>	Read-write	* If labelType is policylabel, name of the policy label to invoke. * If labelType is reqvserver or resvserver, name of the virtual server.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- GET

- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/ videooptimizationpacingpolicylabel_policybinding_binding/ labelname_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ videooptimizationpacingpolicylabel_policybinding_binding/ labelname_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of videooptimizationpacingpolicylabel_policybinding_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ videooptimizationpacingpolicylabel_policybinding_binding/ labelname_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the videooptimizationpacingpolicylabel_policybinding_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "videooptimizationpacingpolicylabel_policybinding_binding": [ {

"priority":<Integer_value>,

"labeltype":<String_value>,

"labelname":<String_value>,

"policyname":<String_value>,

"invoke":<Boolean_value>,

"gotopriorityexpression":<String_value>,

"invoke_labelname":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/ videooptimizationpacingpolicylabel_policybinding_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ videooptimizationpacingpolicylabel_policybinding_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "videooptimizationpacingpolicylabel_policybinding_binding": [ {

"priority":<Integer_value>,

"labeltype":<String_value>,

"labelname":<String_value>,

"policyname":<String_value>,

"invoke":<Boolean_value>,

"gotopriorityexpression":<String_value>,
```

```
"invoke_labelname":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/ videooptimizationpacingpolicylabel_policybinding_binding/ labelname_value<String> ? **count=yes**
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"videooptimizationpacingpolicylabel_policybinding_binding":
[ { "__count": "#no"} ] }
```

videooptimizationpacingpolicylabel_videooptimizationpacingpolicy_binding

Binding object showing the videooptimizationpacingpolicy that can be bound to videooptimizationpacingpolicylabel.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
policyname	<String>	Read-write	Name of the videooptimization policy.
invoke	<Boolean>	Read-write	If the current policy evaluates to TRUE, terminate evaluation of policies bound to the current policy label and evaluate the specified policy label.
gotopriorityexpression	<String>	Read-write	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
invoke_labelname	<String>	Read-write	* If labelType is policylabel, name of the policy label to invoke. * If labelType is reqvserver or resvserver, name of the virtual server.
labelname	<String>	Read-write	Name of the videooptimization pacing policy label to which to bind the policy.
priority	<Integer>	Read-write	Specifies the priority of the policy.
labeltype	<String>	Read-write	Type of policy label to invoke. Available settings function as

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			follows: * vserver - Invoke an unnamed policy label associated with a virtual server. * policylabel - Invoke a user-defined policy label. Possible values = vserver, policylabel
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/ videooptimizationpacingpolicylabel_videooptimizationpacingpolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"videooptimizationpacingpolicylabel_videooptimizationpacingpolicy_binding"
:{

<b>"labelname":<String_value>,

</b><b>"policyname":<String_value>,

</b><b>"priority":<Integer_value>,

</b>"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>,

"labeltype":<String_value>,

"invoke_labelname":<String_value>
```

```
}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/ videooptimizationpacingpolicylabel_videooptimizationpacingpolicy_binding/ labelname_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ videooptimizationpacingpolicylabel_videooptimizationpacingpolicy_binding/ labelname_value<String> ? **args= policyname:<String_value>, priority: <Integer_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/ videooptimizationpacingpolicylabel_videooptimizationpacingpolicy_binding/ labelname_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ videooptimizationpacingpolicylabel_videooptimizationpacingpolicy_binding/ labelname_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of videooptimizationpacingpolicylabel_videooptimizationpacingpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ videooptimizationpacingpolicylabel_videooptimizationpacingpolicy_binding/ labelname_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the videooptimizationpacingpolicylabel_videooptimizationpacingpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "videooptimizationpacingpolicylabel_videooptimizationpacingpolicy_bindi
ng": [ {

"policyname":<String_value>,

"invoke":<Boolean_value>,

"gotopriorityexpression":<String_value>,

"invoke_labelname":<String_value>,

"labelname":<String_value>,

"priority":<Integer_value>,

"labeltype":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/ videooptimizationpacingpolicylabel_videooptimizationpacingpolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ videooptimizationpacingpolicylabel_videooptimizationpacingpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "videooptimizationpacingpolicylabel_videooptimizationpacingpolicy_bindi
ng": [ {

"policyname":<String_value>,

"invoke":<Boolean_value>,

"gotopriorityexpression":<String_value>,

"invoke_labelname":<String_value>,

"labelname":<String_value>,

"priority":<Integer_value>,

"labeltype":<String_value>
```

```
}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/ videooptimizationpacingpolicylabel_videooptimizationpacingpolicy_binding/ labelname_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"videooptimizationpacingpolicylabel_videooptimizationpacingpolicy_binding
": [ { "__count": "#no"} ] }
```

videooptimizationparameter

Configuration for VideoOptimization parameter resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
randomsamplingpercentage	<Double>	Read-write	Random Sampling Percentage. Default value: 0

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum value = 0 Maximum value = 100
quicpacingrate	<Integer>	Read-write	QUIC Video Pacing Rate (Kbps). Minimum value = 0 Maximum value = 2147483647
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- UPDATE
- UNSET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/videooptimizationparameter **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"videooptimizationparameter":{

"randomsamplingpercentage":<Double_value>,

"quicpacingrate":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/videooptimizationparameter? **action=unset** **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"videooptimizationparameter":{

"randomsamplingpercentage":true,

"quicpacingrate":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/videooptimizationparameter **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "videooptimizationparameter": [ {

"randomsamplingpercentage":<Double_value>,

"quicpacingrate":<Integer_value>,
```

```
"_nextgenapiresource":<String_value>

}]}
```

vpn

SSL VPN

Virtual Private Network configuration.

NAME	DESCRIPTION
vpnalwaysonprofile	Configuration for AlwyasON profile
vpnclientlessaccesspolicy	Configuration for Clientless VPN rewrite policy
vpnclientlessaccesspolicy_binding	Binding object showing the resources that can be bound to vpnclientlessaccesspolicy
vpnclientlessaccesspolicy_vpnglobal_binding	Binding object showing the vpnglobal that can be bound to vpnclientlessaccesspolicy
vpnclientlessaccesspolicy_vpnvserver_binding	Binding object showing the vpnvserver that can be bound to vpnclientlessaccesspolicy
vpnclientlessaccessprofile	Configuration for Clientless VPN rewrite profile
vpnepaprofile	Configuration for Epa profile
vpneula	Configuration for EULA for vservers

NAME	DESCRIPTION
vpnformssoaction	Configuration for Form sso action
vpnglobal_appcontroller_binding	Binding object showing the appcontroller that can be bound to vpnglobal
vpnglobal_appfwpolicy_binding	Binding object showing the appfwpolicy that can be bound to vpnglobal
vpnglobal_auditnslogpolicy_binding	Binding object showing the auditnslogpolicy that can be bound to vpnglobal
vpnglobal_auditsyslogpolicy_binding	Binding object showing the auditsyslogpolicy that can be bound to vpnglobal
vpnglobal_authenticationcertpolicy_binding	Binding object showing the authenticationcertpolicy that can be bound to vpnglobal
vpnglobal_authenticationldappolicy_binding	Binding object showing the authenticationldappolicy that can be bound to vpnglobal
vpnglobal_authenticationlocalpolicy_binding	Binding object showing the authenticationlocalpolicy that can be bound to vpnglobal
vpnglobal_authenticationnegotiatepolicy_binding	Binding object showing the authenticationnegotiatepolicy that can be bound to vpnglobal

NAME	DESCRIPTION
vpnglobal_authenticationpolicy_binding	Binding object showing the authenticationpolicy that can be bound to vpnglobal
vpnglobal_authenticationradiuspolicy_binding	Binding object showing the authenticationradiuspolicy that can be bound to vpnglobal
vpnglobal_authenticationsamlpolicy_binding	Binding object showing the authenticationsamlpolicy that can be bound to vpnglobal
vpnglobal_authenticationtacacspolicy_binding	Binding object showing the authenticationtacacspolicy that can be bound to vpnglobal
vpnglobal_binding	Binding object showing the resources that can be bound to vpnglobal
vpnglobal_domain_binding	Binding object showing the domain that can be bound to vpnglobal
vpnglobal_intranetip6_binding	Binding object showing the intranetip6 that can be bound to vpnglobal
vpnglobal_intranetip_binding	Binding object showing the intranetip that can be bound to vpnglobal
vpnglobal_secureprivateaccessurl_binding	Binding object showing the secureprivateaccessurl that can be bound to vpnglobal

NAME	DESCRIPTION
vpnglobal_sharefileserver_binding	Binding object showing the sharefileserver that can be bound to vpnglobal
vpnglobal_sslcertkey_binding	Binding object showing the sslcertkey that can be bound to vpnglobal
vpnglobal_staserver_binding	Binding object showing the staserver that can be bound to vpnglobal
vpnglobal_vpnclientlessaccesspolicy_binding	Binding object showing the vpnclientlessaccesspolicy that can be bound to vpnglobal
vpnglobal_vpneula_binding	Binding object showing the vpneula that can be bound to vpnglobal
vpnglobal_vpnintranetapplication_binding	Binding object showing the vpnintranetapplication that can be bound to vpnglobal
vpnglobal_vpnnexthopserver_binding	Binding object showing the vpnnexthopserver that can be bound to vpnglobal
vpnglobal_vpnportaltheme_binding	Binding object showing the vpnportaltheme that can be bound to vpnglobal
vpnglobal_vpnsecureprivateaccessprofile_binding	Binding object showing the vpnsecureprivateaccessprofile that can be bound to vpnglobal

NAME	DESCRIPTION
vpnglobal_vpnsessionpolicy_binding	Binding object showing the vpnsessionpolicy that can be bound to vpnglobal
vpnglobal_vpntrafficpolicy_binding	Binding object showing the vpntrafficpolicy that can be bound to vpnglobal
vpnglobal_vpnurl_binding	Binding object showing the vpnurl that can be bound to vpnglobal
vpnglobal_vpnurlpolicy_binding	Binding object showing the vpnurlpolicy that can be bound to vpnglobal
vpnicaconnection	Configuration for active ica connections
vpnicadtlsconnection	Configuration for active ica connections
vpnintranetapplication	Configuration for SSLVPN intranet application
vpnnexthopserver	Configuration for Next Hop Server
vpnparameter	Configuration for VPN parameter
vpnpcoipconnection	Configuration for PCoIP connection
vpnpcoipprofile	Configuration for PCoIP session profile
vpnpcoipvserverprofile	Configuration for PCoIP vserver profile
vpnportaltheme	Configuration for portaltheme

NAME	DESCRIPTION
vpnsamlssoprofile	Configuration for SAML sso action
vpnsecureprivateaccessprofile	Configuration for Secure Private Access Profile
vpnsessionaction	Configuration for VPN session action
vpnsessionpolicy	Configuration for VPN session policy
vpnsessionpolicy_aaagroup_binding	Binding object showing the aaagroup that can be bound to vpnsessionpolicy
vpnsessionpolicy_aaauser_binding	Binding object showing the aaauser that can be bound to vpnsessionpolicy
vpnsessionpolicy_binding	Binding object showing the resources that can be bound to vpnsessionpolicy
vpnsessionpolicy_vpnglobal_binding	Binding object showing the vpnglobal that can be bound to vpnsessionpolicy
vpnsessionpolicy_vpnvserver_binding	Binding object showing the vpnvserver that can be bound to vpnsessionpolicy
vpnsfconfig	Configuration for Create a StoreFront configuration file
vpnstoreinfo	Configuration for Store information for a URL
vpntrafficaction	Configuration for VPN traffic action

NAME	DESCRIPTION
vpntrafficpolicy	Configuration for VPN traffic policy
vpntrafficpolicy_aaagroup_binding	Binding object showing the aaagroup that can be bound to vpntrafficpolicy
vpntrafficpolicy_aaauser_binding	Binding object showing the aaauser that can be bound to vpntrafficpolicy
vpntrafficpolicy_binding	Binding object showing the resources that can be bound to vpntrafficpolicy
vpntrafficpolicy_vpnglobal_binding	Binding object showing the vpnglobal that can be bound to vpntrafficpolicy
vpntrafficpolicy_vpnvserver_binding	Binding object showing the vpnvserver that can be bound to vpntrafficpolicy
vpnurl	Configuration for VPN URL
vpnurlaction	Configuration for VPN url action
vpnurlpolicy	Configuration for VPN url policy
vpnurlpolicy_aaagroup_binding	Binding object showing the aaagroup that can be bound to vpnurlpolicy
vpnurlpolicy_aaauser_binding	Binding object showing the aaauser that can be bound to vpnurlpolicy
vpnurlpolicy_binding	Binding object showing the resources that can be bound to vpnurlpolicy

NAME	DESCRIPTION
vpnurlpolicy_vpnglobal_binding	Binding object showing the vpnglobal that can be bound to vpnurlpolicy
vpnurlpolicy_vpnvserver_binding	Binding object showing the vpnvserver that can be bound to vpnurlpolicy
vpnvserver	Configuration for VPN virtual server
vpnvserver_aaapreauthenticationpolicy_binding	Binding object showing the aaapreauthenticationpolicy that can be bound to vpnvserver
vpnvserver_analyticsprofile_binding	Binding object showing the analyticsprofile that can be bound to vpnvserver
vpnvserver_appcontroller_binding	Binding object showing the appcontroller that can be bound to vpnvserver
vpnvserver_appflowpolicy_binding	Binding object showing the appflowpolicy that can be bound to vpnvserver
vpnvserver_appfwpolicy_binding	Binding object showing the appfwpolicy that can be bound to vpnvserver
vpnvserver_auditnslogpolicy_binding	Binding object showing the auditnslogpolicy that can be bound to vpnvserver
vpnvserver_auditsyslogpolicy_binding	Binding object showing the auditsyslogpolicy that can be bound to vpnvserver

NAME	DESCRIPTION
vpnvserver_authenticationcertpolicy_binding	Binding object showing the authenticationcertpolicy that can be bound to vpnvserver
vpnvserver_authenticationdfapolicy_binding	Binding object showing the authenticationdfapolicy that can be bound to vpnvserver
vpnvserver_authenticationldappolicy_binding	Binding object showing the authenticationldappolicy that can be bound to vpnvserver
vpnvserver_authenticationlocalpolicy_binding	Binding object showing the authenticationlocalpolicy that can be bound to vpnvserver
vpnvserver_authenticationloginschemapolicy_binding	Binding object showing the authenticationloginschemapolicy that can be bound to vpnvserver
vpnvserver_authenticationnegotiatepolicy_binding	Binding object showing the authenticationnegotiatepolicy that can be bound to vpnvserver
vpnvserver_authenticationoauthidppolicy_binding	Binding object showing the authenticationoauthidppolicy that can be bound to vpnvserver
vpnvserver_authenticationpolicy_binding	Binding object showing the authenticationpolicy that can be bound to vpnvserver

NAME	DESCRIPTION
vpnvserver_authenticationradiuspolicy_binding	Binding object showing the authenticationradiuspolicy that can be bound to vpnvserver
vpnvserver_authenticationsamlidppolicy_binding	Binding object showing the authenticationsamlidppolicy that can be bound to vpnvserver
vpnvserver_authenticationsamlpolicy_binding	Binding object showing the authenticationsamlpolicy that can be bound to vpnvserver
vpnvserver_authenticationtacacspolicy_binding	Binding object showing the authenticationtacacspolicy that can be bound to vpnvserver
vpnvserver_authenticationwebauthpolicy_binding	Binding object showing the authenticationwebauthpolicy that can be bound to vpnvserver
vpnvserver_binding	Binding object showing the resources that can be bound to vpnvserver
vpnvserver_cachepolicy_binding	Binding object showing the cachepolicy that can be bound to vpnvserver
vpnvserver_cspolicy_binding	Binding object showing the cspolicy that can be bound to vpnvserver
vpnvserver_feopolicy_binding	Binding object showing the feopolicy that can be bound to vpnvserver

NAME	DESCRIPTION
vpnvserver_icapolicy_binding	Binding object showing the icapolicy that can be bound to vpnvserver
vpnvserver_intranetip6_binding	Binding object showing the intranetip6 that can be bound to vpnvserver
vpnvserver_intranetip_binding	Binding object showing the intranetip that can be bound to vpnvserver
vpnvserver_responderpolicy_binding	Binding object showing the responderpolicy that can be bound to vpnvserver
vpnvserver_rewritepolicy_binding	Binding object showing the rewritepolicy that can be bound to vpnvserver
vpnvserver_secureprivateaccessurl_binding	Binding object showing the secureprivateaccessurl that can be bound to vpnvserver
vpnvserver_sharefileserver_binding	Binding object showing the sharefileserver that can be bound to vpnvserver
vpnvserver_staserver_binding	Binding object showing the staserver that can be bound to vpnvserver
vpnvserver_vpnclientlessaccesspolicy_binding	Binding object showing the vpnclientlessaccesspolicy that can be bound to vpnvserver
vpnvserver_vpnepaprofile_binding	Binding object showing the vpnepaprofile that can be bound to vpnvserver

NAME	DESCRIPTION
vpnvserver_vpneula_binding	Binding object showing the vpneula that can be bound to vpnvserver
vpnvserver_vpnintranetapplication_binding	Binding object showing the vpnintranetapplication that can be bound to vpnvserver
vpnvserver_vpnnexthopserver_binding	Binding object showing the vpnnexthopserver that can be bound to vpnvserver
vpnvserver_vpnportaltheme_binding	Binding object showing the vpnportaltheme that can be bound to vpnvserver
vpnvserver_vpnsecureprivateaccessprofile_binding	Binding object showing the vpnsecureprivateaccessprofile that can be bound to vpnvserver
vpnvserver_vpnsessionpolicy_binding	Binding object showing the vpnsessionpolicy that can be bound to vpnvserver
vpnvserver_vpntrafficpolicy_binding	Binding object showing the vpntrafficpolicy that can be bound to vpnvserver
vpnvserver_vpnurl_binding	Binding object showing the vpnurl that can be bound to vpnvserver
vpnvserver_vpnurlpolicy_binding	Binding object showing the vpnurlpolicy that can be bound to vpnvserver

vpnalwaysonprofile

Configuration for AlwyasON profile resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	name of AlwaysON profile. Minimum length = 1
networkaccessonvpnfailure	<String>	Read-write	Option to block network traffic when tunnel is not established(and the config requires that tunnel be established). When set to onlyToGateway, the network traffic to and from the client (except Gateway IP) is blocked. When set to fullAccess, the network traffic is not blocked. Default value: fullAccess, Possible values = onlyToGateway, fullAccess
clientcontrol	<String>	Read-write	Allow/Deny user to log off and connect to another Gateway. Default value: DENY Possible values = ALLOW, DENY

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
locationbasedvpn	<String>	Read-write	Option to decide if tunnel should be established when in enterprise network. When locationBasedVPN is remote, client tries to detect if it is located in enterprise network or not and establishes the tunnel if not in enterprise network. Dns suffixes configured using -add dns suffix- are used to decide if the client is in the enterprise network or not. If the resolution of the DNS suffix results in private IP, client is said to be in enterprise network. When set to EveryWhere, the client skips the check to detect if it is on the enterprise network and tries to establish the tunnel. Default value: Remote Possible values = Remote, Everywhere
_nextgenapiresource	<String>	Read-only	.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnalwaysonprofile **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"vpnalwaysonprofile":{

<b>"name":<String_value>,

</b>"networkaccessonvpnfailure":<String_value>,

"clientcontrol":<String_value>,

"locationbasedvpn":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnalwaysonprofile/ name_value<String>
HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnalwaysonprofile **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"vpnalwaysonprofile":{

<b>"name":<String_value>,

</b>"networkaccessonvpnfailure":<String_value>,

"clientcontrol":<String_value>,

"locationbasedvpn":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnalwaysonprofile? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"vpnalwaysonprofile":{

<b>"name":<String_value>,

</b>"networkaccessonvpnfailure":true,

"clientcontrol":true,

"locationbasedvpn":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnalwaysonprofile **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/vpnalwaysonprofile? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/vpnalwaysonprofile? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of vpnalwaysonprofile resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/vpnalwaysonprofile? **view=summary**

Use this query-parameter to get the summary output of vpnalwaysonprofile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/vpnalwaysonprofile? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vpnalwaysonprofile resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vpnalwaysonprofile": [ {

"name":<String_value>,

"networkaccessonvpnfailure":<String_value>,

"clientcontrol":<String_value>,

"locationbasedvpn":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnalwaysonprofile/ name_value<String>
Query-parameters: attrs http:// <netscaler-ip-address> /nitro/v1/config/vpnalwaysonprofile/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/vpnalwaysonprofile/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of vpnalwaysonprofile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnalwaysonprofile": [ {

"name":<String_value>,

"networkaccessonvpnfailure":<String_value>,

"clientcontrol":<String_value>,

"locationbasedvpn":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnalwaysonprofile? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vpnalwaysonprofile": [ { "__count": "#no"} ] }
```

vpnclientlessaccesspolicy

Configuration for Clientless VPN rewrite policy resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the new clientless access policy. Minimum length = 1
rule	<String>	Read-write	Expression, or name of a named expression, specifying the traffic that matches the policy. The following requirements apply only to the Citrix ADC CLI:

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			* If the expression includes one or more spaces, enclose the entire expression in double quotation marks. * If the expression itself includes double quotation marks, escape the quotations by using the \ character. * Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks.
profilename	<String>	Read-write	Name of the profile to invoke for the clientless access.
undefaction	<String>	Read-only	The UNDEF action.
hits	<Integer>	Read-only	The number of times the policy evaluated to true.
undefhits	<Integer>	Read-only	The number of times the policy evaluation resulted in undefined processing.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
description	<String>	Read-only	Description of the clientless access policy.
isdefault	<Boolean>	Read-only	A value of true is returned if it is a default vpnclientlessrwpolicy .
builtin	<String[]>	Read-only	Flag to determine if vpn clientless rewrite policy is built-in or not. Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL
feature	<String>	Read-only	The feature to be checked while applying this config.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnclientlessaccesspolicy **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"vpnclientlessaccesspolicy":{

<b>"name":<String_value>,
```

```
</b><b>"rule":<String_value>,

</b><b>"profilename":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnclientlessaccesspolicy/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnclientlessaccesspolicy **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"vpnclientlessaccesspolicy":{

<b>"name":<String_value>,

</b>"rule":<String_value>,

"profilename":<String_value>
```

```
}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnclientlessaccesspolicy **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/vpnclientlessaccesspolicy? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/vpnclientlessaccesspolicy? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of vpnclientlessaccesspolicy resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/vpnclientlessaccesspolicy? **view=summary**

Use this query-parameter to get the summary output of vpnclientlessaccesspolicy resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/vpnclientlessaccesspolicy? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vpnclientlessaccesspolicy resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vpnclientlessaccesspolicy": [ {

"name":<String_value>,

"rule":<String_value>,

"profilename":<String_value>,

"undefaction":<String_value>,

"hits":<Integer_value>,

"undefhits":<Integer_value>,

"description":<String_value>,

"isdefault":<Boolean_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnclientlessaccesspolicy/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/ vpnclientlessaccesspolicy/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/vpnclientlessaccesspolicy/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of vpnclientlessaccesspolicy resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnclientlessaccesspolicy": [ {

"name":<String_value>,

"rule":<String_value>,

"profilename":<String_value>,

"undefaction":<String_value>,

"hits":<Integer_value>,

"undefhits":<Integer_value>,

"description":<String_value>,

"isdefault":<Boolean_value>,
```

```
"builtin":<String[]_value>,

"feature":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnclientlessaccesspolicy? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vpnclientlessaccesspolicy": [ { "__count": "#no"} ] }
```

vpnclientlessaccesspolicy_binding

Binding object which returns the resources bound to vpnclientlessaccesspolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the clientless access policy to display. Minimum length = 1
vpnclientlessaccesspolicy_vpnvserver_binding	<vpnclientlessaccesspolicy_vpnvserver_binding[]>	Read-only	vpnvserver that can be bound to vpnclientlessaccesspolicy.
vpnclientlessaccesspolicy_vpnglobal_binding	<vpnclientlessaccesspolicy_vpnglobal_binding[]>	Read-only	vpnglobal that can be bound to vpnclientlessaccesspolicy.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnclientlessaccesspolicy_binding/ name_value<String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vpnclientlessaccesspolicy_binding": [ {

"name":<String_value>,

"vpnclientlessaccesspolicy_vpnvserver_binding":<vpnclientlessaccesspolicy_
vpnvserver_binding[]_value>,

"vpnclientlessaccesspolicy_vpnglobal_binding":<vpnclientlessaccesspolicy_v
pnglobal_binding[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnclientlessaccesspolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/vpnclientlessaccesspolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vpnclientlessaccesspolicy_binding": [ {

"name":<String_value>,

"vpnclientlessaccesspolicy_vpnvserver_binding":<vpnclientlessaccesspolicy_
vpnvserver_binding[]_value>,

"vpnclientlessaccesspolicy_vpnglobal_binding":<vpnclientlessaccesspolicy_v
pnglobal_binding[]_value>

}]}
```

vpnclientlessaccesspolicy_vpnglobal_binding

Binding object showing the vpnglobal that can be bound to vpnclientlessaccesspolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
boundto	<String>	Read-write	Location where policy is bound.
name	<String>	Read-write	Name of the clientless access policy to display. Minimum length = 1
priority	<Integer>	Read-only	Specifies the priority of the policy. Minimum value = 1 Maximum value = 2147483647
activepolicy	<Integer>	Read-only	Indicates whether policy is bound or not.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnclientlessaccesspolicy_vpnglobal_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ vpnclientlessaccesspolicy_vpnglobal_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of vpnclientlessaccesspolicy_vpnglobal_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ vpnclientlessaccesspolicy_vpnglobal_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vpnclientlessaccesspolicy_vpnglobal_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnclientlessaccesspolicy_vpnglobal_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"priority":<Integer_value>,

"activepolicy":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnclientlessaccesspolicy_vpnglobal_binding
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/vpnclientlessaccesspolicy_vpnglobal_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnclientlessaccesspolicy_vpnglobal_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"priority":<Integer_value>,

"activepolicy":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnclientlessaccesspolicy_vpnglobal_binding/name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"vpnclientlessaccesspolicy_vpnglobal_binding": [ { "__count": "#no"} ] }
```

vpnclientlessaccesspolicy_vpnvserver_binding

Binding object showing the vpnvserver that can be bound to vpnclientlessaccesspolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the clientless access policy to display. Minimum length = 1
boundto	<String>	Read-write	Location where policy is bound.
activepolicy	<Integer>	Read-only	Indicates whether policy is bound or not.
priority	<Integer>	Read-only	Specifies the priority of the policy. Minimum value = 1 Maximum value = 2147483647
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnclientlessaccesspolicy_vpnvserver_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ vpnclientlessaccesspolicy_vpnvserver_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of vpnclientlessaccesspolicy_vpnvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ vpnclientlessaccesspolicy_vpnvserver_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vpnclientlessaccesspolicy_vpnvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnclientlessaccesspolicy_vpnvserver_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"activepolicy":<Integer_value>,

"priority":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnclientlessaccesspolicy_vpnvserver_binding
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/vpnclientlessaccesspolicy_vpnvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnclientlessaccesspolicy_vpnvserver_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"activepolicy":<Integer_value>,

"priority":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnclientlessaccesspolicy_vpnvserver_binding/name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"vpnclientlessaccesspolicy_vpnvserver_binding": [ { "__count": "#no"} ] }
```

vpnclientlessaccessprofile

Configuration for Clientless VPN rewrite profile resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
profilename	<String>	Read-write	Name for the Citrix Gateway clientless access profile. Must begin with an ASCII alphabetic or underscore (_) character, and must consist only of ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the profile is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			"my profile" or 'my profile'). Minimum length = 1
urlrewritepolicylabel	<String>	Read-write	Name of the configured URL rewrite policy label. If you do not specify a policy label name, then URLs are not rewritten. Minimum length = 1
javascriptrewritepolicylabel	<String>	Read-write	Name of the configured JavaScript rewrite policy label. If you do not specify a policy label name, then JAVA scripts are not rewritten. Minimum length = 1
reqhdrrewritepolicylabel	<String>	Read-write	Name of the configured Request rewrite policy label. If you do not specify a policy label name, then requests are not rewritten. Minimum length = 1
reshdrrewritepolicylabel	<String>	Read-write	Name of the configured Response rewrite policy label. Minimum length = 1
regexforfindingurlinjavascript	<String>	Read-write	Name of the pattern set that contains the regular expressions,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			which match the URL in Java script. Minimum length = 1
regexforfindingurlincss	<String>	Read-write	Name of the pattern set that contains the regular expressions, which match the URL in the CSS. Minimum length = 1
regexforfindingurlinxcomponent	<String>	Read-write	Name of the pattern set that contains the regular expressions, which match the URL in X Component. Minimum length = 1
regexforfindingurlinxml	<String>	Read-write	Name of the pattern set that contains the regular expressions, which match the URL in XML. Minimum length = 1
regexforfindingcustomurls	<String>	Read-write	Name of the pattern set that contains the regular expressions, which match the URLs in the custom content type other than HTML, CSS, XML, XCOMP, and JavaScript. The custom content type should be included in the patset ns_cvpn_custom_content_types.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum length = 1
clientconsumedcookies	<String>	Read-write	Specify the name of the pattern set containing the names of the cookies, which are allowed between the client and the server. If a pattern set is not specified, Citrix Gateway does not allow any cookies between the client and the server. A cookie that is not specified in the pattern set is handled by Citrix Gateway on behalf of the client. Minimum length = 1
requirepersistentcookie	<String>	Read-write	Specify whether a persistent session cookie is set and accepted for clientless access. If this parameter is set to ON, COM objects, such as MSOffice, which are invoked by the browser can access the files using clientless access. Use caution because the persistent cookie is stored on the disk. Default value: OFF

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ON, OFF
cssrewritepolicylabel	<String>	Read-only	The configured CSS rewrite policylabel. Minimum length = 1
xmlrewritepolicylabel	<String>	Read-only	The configured XML rewrite policylabel. Minimum length = 1
xcomponentrewritepolicylabel	<String>	Read-only	The configured X-Component rewrite policylabel. Minimum length = 1
isdefault	<Boolean>	Read-only	A value of true is returned if it is a default vpnclientlessrwprofile.
description	<String>	Read-only	Description of the clientless access profile.
builtin	<String[]>	Read-only	Flag to determine if vpn clientless rewrite profile is built-in or not. Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL
feature	<String>	Read-only	The feature to be checked while applying this config.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnclientlessaccessprofile **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"vpnclientlessaccessprofile":{

<b>"profilename":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnclientlessaccessprofile/profilename_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnclientlessaccessprofile **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"vpnclientlessaccessprofile":{

<b>"profilename":<String_value>,

</b>"urlrewritepolicylabel":<String_value>,

"javascriptrewritepolicylabel":<String_value>,

"reqhdrrewritepolicylabel":<String_value>,

"reshdrrewritepolicylabel":<String_value>,

"regexforfindingurlinjavascript":<String_value>,

"regexforfindingurlincss":<String_value>,

"regexforfindingurlinxcomponent":<String_value>,

"regexforfindingurlinxml":<String_value>,

"regexforfindingcustomurls":<String_value>,

"clientconsumedcookies":<String_value>,

"requirepersistentcookie":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnclientlessaccessprofile? **action=unset**

HTTP Method: POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"vpnclientlessaccessprofile":{

<b>"profilename":<String_value>,

</b>"urlrewritepolicylabel":true,

"javascriptrewritepolicylabel":true,

"reqhdrrewritepolicylabel":true,

"reshdrrewritepolicylabel":true,

"regexforfindingurlinjavascript":true,

"regexforfindingurlincss":true,

"regexforfindingurlinxcomponent":true,

"regexforfindingurlinxml":true,

"regexforfindingcustomurls":true,

"clientconsumedcookies":true,

"requirepersistentcookie":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnclientlessaccessprofile **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/vpnclientlessaccessprofile? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/vpnclientlessaccessprofile? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of vpnclientlessaccessprofile resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/vpnclientlessaccessprofile? **view=summary**

Use this query-parameter to get the summary output of vpnclientlessaccessprofile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/vpnclientlessaccessprofile? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vpnclientlessaccessprofile resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vpnclientlessaccessprofile": [ {

"profilename":<String_value>,

"urlrewritepolicylabel":<String_value>,

"javascriptrewritepolicylabel":<String_value>,

"cssrewritepolicylabel":<String_value>,

"xmlrewritepolicylabel":<String_value>,

"xcomponentrewritepolicylabel":<String_value>,

"reqhdrrewritepolicylabel":<String_value>,

"reshdrrewritepolicylabel":<String_value>,

"regexforfindingurlinjavascript":<String_value>,

"regexforfindingurlincss":<String_value>,

"regexforfindingurlinxcomponent":<String_value>,

"regexforfindingurlinxml":<String_value>,

"regexforfindingcustomurls":<String_value>,

"clientconsumedcookies":<String_value>,

"requirepersistentcookie":<String_value>,

"isdefault":<Boolean_value>,

"description":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"_nextgenapiresource":<String_value>
```

```
}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnclientlessaccessprofile/ profilename_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/ config/vpnclientlessaccessprofile/ profilename_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/vpnclientlessaccessprofile/ profilename_value<String> ? **view=summary**

Use this query-parameter to get the summary output of vpnclientlessaccessprofile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnclientlessaccessprofile": [ {

"profilename":<String_value>,

"urlrewritepolicylabel":<String_value>,
```

```
"javascriptrewritepolicylabel":<String_value>,

"cssrewritepolicylabel":<String_value>,

"xmlrewritepolicylabel":<String_value>,

"xcomponentrewritepolicylabel":<String_value>,

"reqhdrrewritepolicylabel":<String_value>,

"reshdrrewritepolicylabel":<String_value>,

"regexforfindingurlinjavascript":<String_value>,

"regexforfindingurlincss":<String_value>,

"regexforfindingurlinxcomponent":<String_value>,

"regexforfindingurlinxml":<String_value>,

"regexforfindingcustomurls":<String_value>,

"clientconsumedcookies":<String_value>,

"requirepersistentcookie":<String_value>,

"isdefault":<Boolean_value>,

"description":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnclientlessaccessprofile? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vpnclientlessaccessprofile": [ { "__count": "#no"} ] }
```

vpnepaprofile

Configuration for Epa profile resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	name of device profile. Minimum length = 1
filename	<String>	Read-write	filename of the deviceprofile data xml. Minimum length = 1
data	<String>	Read-write	deviceprofile data xml. Minimum length = 1
_nextgenapiresource	<String>	Read-only	.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnepaprofile **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"vpnepaprofile":{

<b>"name":<String_value>,

</b>"filename":<String_value>,

"data":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnepaprofile/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnepaprofile **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/vpnepaprofile? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/vpnepaprofile? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of vpnepaprofile resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/vpnepaprofile? **view=summary**

Use this query-parameter to get the summary output of vpnepaprofile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/vpnepaprofile? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vpnepaprofile resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vpnepaprofile": [ {

"name":<String_value>,

"data":<String_value>,
```

```
"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnepaprofile/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/vpnepaprofile/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/vpnepaprofile/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of vpnepaprofile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnepaprofile": [ {

"name":<String_value>,
```

```
"data":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnepaprofile? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vpnepaprofile": [ { "__count": "#no"} ] }
```

vpneula

Configuration for EULA for vservers resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the eula. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpneula **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"vpneula":{

<b>"name":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpneula/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpneula **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/vpneula? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/vpneula? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of vpneula resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/vpneula? **view=summary**

Use this query-parameter to get the summary output of vpneula resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/vpneula? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vpneula resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vpneula": [ {

"name":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpneula/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/vpneula/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/vpneula/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of vpneula resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpneula": [ {

"name":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpneula? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vpneula": [ { "__count": "#no"} ] }
```

vpnformssoaction

Configuration for Form sso action resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the form based single sign-on profile. Minimum length = 1
actionurl	<String>	Read-write	Root-relative URL to which the completed form is submitted. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
userfield	<String>	Read-write	Name of the form field in which the user types in the user ID. Minimum length = 1
passwdfield	<String>	Read-write	Name of the form field in which the user types in the password. Minimum length = 1
ssosuccessrule	<String>	Read-write	Expression that defines the criteria for SSO success. Expression such as checking for cookie in the response is a common example.
namevaluepair	<String>	Read-write	Other name-value pair attributes to send to the server, in addition to sending the user name and password. Value names are separated by an ampersand (;), such as in name1=value1;name2=value2.
responsesize	<Integer>	Read-write	Maximum number of bytes to allow in the response size. Specifies the number of bytes in the response to be parsed for extracting the forms.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: 8096
nvtype	<String>	Read-write	How to process the name-value pair. Available settings function as follows: * STATIC - The administrator-configured values are used. * DYNAMIC - The response is parsed, the form is extracted, and then submitted. Default value: DYNAMIC Possible values = STATIC, DYNAMIC
submitmethod	<String>	Read-write	HTTP method (GET or POST) used by the single sign-on form to send the logon credentials to the logon server. Default value: GET Possible values = GET, POST
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnformssoaction **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"vpnformssoaction":{

<b>"name":<String_value>,

</b><b>"actionurl":<String_value>,

</b><b>"userfield":<String_value>,

</b><b>"passwdfield":<String_value>,

</b><b>"ssosuccessrule":<String_value>,

</b>"namevaluepair":<String_value>,

"responsesize":<Integer_value>,

"nvtype":<String_value>,

"submitmethod":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnformssoaction/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnformssoaction **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"vpnformssoaction":{

<b>"name":<String_value>,

</b>"actionurl":<String_value>,

"userfield":<String_value>,

"passwdfield":<String_value>,

"ssosuccessrule":<String_value>,

"responsesize":<Integer_value>,

"namevaluepair":<String_value>,

"nvtype":<String_value>,

"submitmethod":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnformssoaction? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"vpnformssoaction":{

<b>"name":<String_value>,

</b>"responsesize":true,

"namevaluepair":true,

"nvtype":true,

"submitmethod":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnformssoaction **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/vpnformssoaction? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/vpnformssoaction? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of vpnformssoaction resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/vpnformssoaction? **view=summary**

Use this query-parameter to get the summary output of vpnformssoaction resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/vpnformssoaction? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vpnformssoaction resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vpnformssoaction": [ {

"name":<String_value>,

"actionurl":<String_value>,

"userfield":<String_value>,

"passwdfield":<String_value>,

"responsesize":<Integer_value>,
```

```
"namevaluepair":<String_value>,

"nvtype":<String_value>,

"ssosuccessrule":<String_value>,

"submitmethod":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnformssoaction/ name_value<String>
Query-parameters: attrs http:// <netscaler-ip-address> /nitro/v1/config/vpnformssoaction/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/vpnformssoaction/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of vpnformssoaction resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnformssoaction": [ {

"name":<String_value>,

"actionurl":<String_value>,

"userfield":<String_value>,

"passwdfield":<String_value>,

"responsesize":<Integer_value>,

"namevaluepair":<String_value>,

"nvtype":<String_value>,

"ssosuccessrule":<String_value>,

"submitmethod":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnformssoaction? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vpnformssoaction": [ { "__count": "#no"} ] }
```

vpnglobal_appcontroller_binding

Binding object showing the appcontroller that can be bound to vpnglobal.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
gotopriorityexpression	<String>	Read-write	Applicable only to advance vpn session policy. An expression or other value specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
appcontroller	<String>	Read-write	Configured App Controller server.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/vpnglobal_appcontroller_binding

HTTP Method: PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"vpnglobal_appcontroller_binding":{
```

```
"appcontroller":<String_value>,

"gotopriorityexpression":<String_value>

}}
```

Response:

HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_appcontroller_binding

Query-parameters:

args

http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_appcontroller_binding?
args=appcontroller: <String_value>

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_appcontroller_binding

Query-parameters:

filter

http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_appcontroller_binding? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of vpnglobal_appcontroller_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination

http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_appcontroller_binding? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vpnglobal_appcontroller_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnglobal_appcontroller_binding": [ {

"gotopriorityexpression":<String_value>,

"appcontroller":<String_value>

}]}
```

```
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_appcontroller_binding? **count=yes**

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vpnglobal_appcontroller_binding": [ { "__count": "#no"} ] }
```

vpnglobal_appfwpolicy_binding

Binding object showing the appfwpolicy that can be bound to vpnglobal.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
policyname	<String>	Read-write	The name of the policy.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
gotopriorityexpression	<String>	Read-write	Applicable only to advance vpn session policy. An expression or other value specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
groupextraction	<Boolean>	Read-write	Bind the Authentication policy to a tertiary chain which will be used only for group extraction. The user will not authenticate against this server, and this will only be called it primary and/or secondary authentication has succeeded.
priority	<Integer>	Read-write	Integer specifying the policy's priority. The lower the priority number, the higher the policy's priority. Maximum value for default syntax policies is 2147483647 and for classic policies is 64000. Minimum value = 0 Maximum value = 2147483647

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
secondary	<Boolean>	Read-write	Bind the authentication policy as the secondary policy to use in a two-factor configuration. A user must then authenticate not only to a primary authentication server but also to a secondary authentication server. User groups are aggregated across both authentication servers. The user name must be exactly the same on both authentication servers, but the authentication servers can require different passwords.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/vpnglobal_appfwpolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"vpnglobal_appfwpolicy_binding":{

"policyname":<String_value>,
```

```
"priority":<Integer_value>,

"secondary":<Boolean_value>,

"groupextraction":<Boolean_value>,

"gotopriorityexpression":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_appfwpolicy_binding **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_appfwpolicy_binding? **args=policyname: <String_value> ,secondary: <Boolean_value> ,groupextraction: <Boolean_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_appfwpolicy_binding **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_appfwpolicy_binding? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of vpnglobal_appfwpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_appfwpolicy_binding? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vpnglobal_appfwpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnglobal_appfwpolicy_binding": [ {

"policyname":<String_value>,

"gotopriorityexpression":<String_value>,

"groupextraction":<Boolean_value>,

"priority":<Integer_value>,

"secondary":<Boolean_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_appfwpolicy_binding? **count=yes**
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vpnglobal_appfwpolicy_binding": [ { "__count": "#no"} ] }
```

vpnglobal_auditnslogpolicy_binding

Binding object showing the auditnslogpolicy that can be bound to vpnglobal.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
groupextraction	<Boolean>	Read-write	Bind the Authentication policy to a tertiary chain which will be used only for group extraction. The user will not authenticate against this server, and this will only be called it primary and/or secondary authentication has succeeded.
policyname	<String>	Read-write	The name of the policy.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
gotopriorityexpression	<String>	Read-write	Applicable only to advance vpn session policy. An expression or other value specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
priority	<Integer>	Read-write	Integer specifying the policy's priority. The lower the priority number, the higher the policy's priority. Maximum value for default syntax policies is 2147483647 and for classic policies is 64000. Minimum value = 0 Maximum value = 2147483647
secondary	<Boolean>	Read-write	Bind the authentication policy as the secondary policy to use in a two-factor configuration. A user must then authenticate not only to a primary authentication server but also to a secondary authentication server. User groups

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			are aggregated across both authentication servers. The user name must be exactly the same on both authentication servers, but the authentication servers can require different passwords.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/vpnglobal_auditnslogpolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"vpnglobal_auditnslogpolicy_binding":{

"policyname":<String_value>,

"priority":<Integer_value>,

"secondary":<Boolean_value>,

"groupextraction":<Boolean_value>,

"gotopriorityexpression":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_auditnslogpolicy_binding **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_auditnslogpolicy_binding? **args=policyname: <String_value> ,secondary: <Boolean_value> ,groupextraction: <Boolean_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_auditnslogpolicy_binding **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_auditnslogpolicy_binding? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of vpnglobal_auditnslogpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_auditnslogpolicy_binding? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vpnglobal_auditnslogpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnglobal_auditnslogpolicy_binding": [ {

"groupextraction":<Boolean_value>,

"policyname":<String_value>,

"gotopriorityexpression":<String_value>,

"priority":<Integer_value>,

"secondary":<Boolean_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_auditnslogpolicy_binding?**count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vpnglobal_auditnslogpolicy_binding": [ { "__count": "#no"} ] }
```

vpnglobal_auditsyslogpolicy_binding

Binding object showing the auditsyslogpolicy that can be bound to vpnglobal.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
secondary	<Boolean>	Read-write	Bind the authentication policy as the secondary policy to use in a two-factor configuration. A user must then authenticate not only to a primary authentication server but also to a secondary authentication server. User groups are aggregated across both authentication servers. The user name must be exactly the same on both authentication servers, but the authentication servers can require different passwords.
priority	<Integer>	Read-write	Integer specifying the policy's priority. The lower the priority number, the higher

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			the policy's priority. Maximum value for default syntax policies is 2147483647 and for classic policies is 64000. Minimum value = 0 Maximum value = 2147483647
groupextraction	<Boolean>	Read-write	Bind the Authentication policy to a tertiary chain which will be used only for group extraction. The user will not authenticate against this server, and this will only be called it primary and/or secondary authentication has succeeded.
gotopriorityexpression	<String>	Read-write	Applicable only to advance vpn session policy. An expression or other value specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
policyname	<String>	Read-write	The name of the policy.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/vpnglobal_auditsyslogpolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"vpnglobal_auditsyslogpolicy_binding":{

"policyname":<String_value>,

"priority":<Integer_value>,

"secondary":<Boolean_value>,

"groupextraction":<Boolean_value>,

"gotopriorityexpression":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_auditsyslogpolicy_binding **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_auditsyslogpolicy_binding? **args=policyname: <String_value> ,secondary: <Boolean_value> ,groupextraction: <Boolean_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_auditsyslogpolicy_binding **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_auditsyslogpolicy_binding? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of vpnglobal_auditsyslogpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_auditsyslogpolicy_binding? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vpnglobal_auditsyslogpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnglobal_auditsyslogpolicy_binding": [ {

"secondary":<Boolean_value>,

"priority":<Integer_value>,

"groupextraction":<Boolean_value>,
```

```
"gotopriorityexpression":<String_value>,

"policyname":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_auditsyslogpolicy_binding? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vpnglobal_auditsyslogpolicy_binding": [ { "__count": "#no"} ] }
```

vpnglobal_authenticationcertpolicy_binding

Binding object showing the authenticationcertpolicy that can be bound to vpnglobal.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
priority	<Integer>	Read-write	Integer specifying the policy's priority.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			The lower the priority number, the higher the policy's priority. Maximum value for default syntax policies is 2147483647 and for classic policies is 64000. Minimum value = 0 Maximum value = 2147483647
secondary	<Boolean>	Read-write	Bind the authentication policy as the secondary policy to use in a two-factor configuration. A user must then authenticate not only to a primary authentication server but also to a secondary authentication server. User groups are aggregated across both authentication servers. The user name must be exactly the same on both authentication servers, but the authentication servers can require different passwords.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
gotopriorityexpression	<String>	Read-write	Applicable only to advance vpn session policy. An expression or other value specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
policyname	<String>	Read-write	The name of the policy.
groupextraction	<Boolean>	Read-write	Bind the Authentication policy to a tertiary chain which will be used only for group extraction. The user will not authenticate against this server, and this will only be called it primary and/or secondary authentication has succeeded.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/vpnglobal_authenticationcertpolicy_binding
HTTP Method: PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"vpnglobal_authenticationcertpolicy_binding":{

"policyname":<String_value>,
```

```
"priority":<Integer_value>,

"secondary":<Boolean_value>,

"groupextraction":<Boolean_value>,

"gotopriorityexpression":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_authenticationcertpolicy_binding **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_authenticationcertpolicy_binding? **args=policyname: <String_value> ,secondary: <Boolean_value> ,groupextraction: <Boolean_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_authenticationcertpolicy_binding **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_authenticationcertpolicy_binding? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of vpnglobal_authenticationcertpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ vpnglobal_authenticationcertpolicy_binding? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vpnglobal_authenticationcertpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnglobal_authenticationcertpolicy_binding": [ {

"priority":<Integer_value>,

"secondary":<Boolean_value>,

"gotopriorityexpression":<String_value>,

"policyname":<String_value>,

"groupextraction":<Boolean_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_authenticationcertpolicy_binding? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vpnglobal_authenticationcertpolicy_binding": [ { "__count": "#no"} ] }
```

vpnglobal_authenticationldappolicy_binding

Binding object showing the authenticationldappolicy that can be bound to vpnglobal.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
groupextraction	<Boolean>	Read-write	Bind the Authentication policy to a tertiary chain which will be used only for group extraction. The user will not authenticate against this server, and this will only be called it primary and/or secondary authentication has succeeded.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
gotopriorityexpression	<String>	Read-write	Applicable only to advance vpn session policy. An expression or other value specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
policyname	<String>	Read-write	The name of the policy.
priority	<Integer>	Read-write	Integer specifying the policy's priority. The lower the priority number, the higher the policy's priority. Maximum value for default syntax policies is 2147483647 and for classic policies is 64000. Minimum value = 0 Maximum value = 2147483647
secondary	<Boolean>	Read-write	Bind the authentication policy as the secondary policy to use in a two-factor configuration. A user must then authenticate not only to a primary authentication server but also to a

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			secondary authentication server. User groups are aggregated across both authentication servers. The user name must be exactly the same on both authentication servers, but the authentication servers can require different passwords.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of

creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/vpnglobal_authenticationldappolicy_binding
HTTP Method: PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"vpnglobal_authenticationldappolicy_binding":{

"policyname":<String_value>,

"priority":<Integer_value>,

"secondary":<Boolean_value>,

"groupextraction":<Boolean_value>,

"gotopriorityexpression":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_authenticationldappolicy_binding **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_authenticationldappolicy_binding? **args=policyname: <String_value> ,secondary: <Boolean_value> ,groupextraction: <Boolean_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_authenticationldappolicy_binding **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_authenticationldappolicy_binding? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of vpnglobal_authenticationldappolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_authenticationldappolicy_binding? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vpnglobal_authenticationldappolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnglobal_authenticationldappolicy_binding": [ {

"groupextraction":<Boolean_value>,

"gotopriorityexpression":<String_value>,

"policyname":<String_value>,

"priority":<Integer_value>,

"secondary":<Boolean_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_authenticationldappolicy_binding? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vpnglobal_authenticationldappolicy_binding": [ { "__count": "#no"} ] }
```

vpnglobal_authenticationlocalpolicy_binding

Binding object showing the authenticationlocalpolicy that can be bound to vpnglobal.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
secondary	<Boolean>	Read-write	Bind the authentication policy as the secondary policy to use in a two-factor configuration. A user must then authenticate not only to a primary authentication server but also to a secondary authentication server. User groups are aggregated across both authentication servers. The user name must be exactly the same on both authentication servers, but the authentication

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			servers can require different passwords.
priority	<Integer>	Read-write	Integer specifying the policy's priority. The lower the priority number, the higher the policy's priority. Maximum value for default syntax policies is 2147483647 and for classic policies is 64000. Minimum value = 0 Maximum value = 2147483647
policyname	<String>	Read-write	The name of the policy.
gotopriorityexpression	<String>	Read-write	Applicable only to advance vpn session policy. An expression or other value specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
groupextraction	<Boolean>	Read-write	Bind the Authentication policy to a tertiary chain which will be used only for group extraction. The user will not authenticate against this server,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			and this will only be called it primary and/ or secondary authentication has succeeded.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/vpnglobal_authenticationlocalpolicy_binding
HTTP Method: PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"vpnglobal_authenticationlocalpolicy_binding":{

"policyname":<String_value>,

"priority":<Integer_value>,

"secondary":<Boolean_value>,

"groupextraction":<Boolean_value>,

"gotopriorityexpression":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_authenticationlocalpolicy_binding
Query-parameters: args http:// <netscaler-ip-address> /nitro/v1/config/

vpnglobal_authenticationlocalpolicy_binding? **args=policyname: <String_value> ,secondary: <Boolean_value> ,groupextraction: <Boolean_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_authenticationlocalpolicy_binding **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_authenticationlocalpolicy_binding? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of vpnglobal_authenticationlocalpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_authenticationlocalpolicy_binding? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vpnglobal_authenticationlocalpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnglobal_authenticationlocalpolicy_binding": [ {

"secondary":<Boolean_value>,

"priority":<Integer_value>,

"policyname":<String_value>,

"gotopriorityexpression":<String_value>,

"groupextraction":<Boolean_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_authenticationlocalpolicy_binding? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vpnglobal_authenticationlocalpolicy_binding": [ { "__count": "#no"} ] }
```

vpnglobal_authenticationnegotiatepolicy_binding

Binding object showing the authenticationnegotiatepolicy that can be bound to vpnglobal.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
groupextraction	<Boolean>	Read-write	Bind the Authentication policy to a tertiary chain which will be used only for group extraction. The user will not authenticate against this server, and this will only be called it primary and/or secondary authentication has succeeded.
policyname	<String>	Read-write	The name of the policy.
gotopriorityexpression	<String>	Read-write	Applicable only to advance vpn session policy. An expression or other value specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
secondary	<Boolean>	Read-write	Bind the authentication policy as the secondary policy to use in a two-factor configuration. A user

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			must then authenticate not only to a primary authentication server but also to a secondary authentication server. User groups are aggregated across both authentication servers. The user name must be exactly the same on both authentication servers, but the authentication servers can require different passwords.
priority	<Integer>	Read-write	Integer specifying the policy's priority. The lower the priority number, the higher the policy's priority. Maximum value for default syntax policies is 2147483647 and for classic policies is 64000. Minimum value = 0 Maximum value = 2147483647
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/vpnglobal_authenticationnegotiatepolicy_binding
HTTP Method: PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"vpnglobal_authenticationnegotiatepolicy_binding":{

"policyname":<String_value>,

"priority":<Integer_value>,

"secondary":<Boolean_value>,

"groupextraction":<Boolean_value>,

"gotopriorityexpression":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/ vpnglobal_authenticationnegotiatepolicy_binding **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_authenticationnegotiatepolicy_binding? **args=policyname: <String_value> ,secondary: <Boolean_value> ,groupextraction: <Boolean_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/ vpnglobal_authenticationnegotiatepolicy_binding **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_authenticationnegotiatepolicy_binding? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of vpnglobal_authenticationnegotiatepolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ vpnglobal_authenticationnegotiatepolicy_binding? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vpnglobal_authenticationnegotiatepolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnglobal_authenticationnegotiatepolicy_binding": [ {

"groupextraction":<Boolean_value>,

"policyname":<String_value>,

"gotopriorityexpression":<String_value>,

"secondary":<Boolean_value>,
```

```
"priority":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/ vpnglobal_authenticationnegotiatepolicy_binding? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vpnglobal_authenticationnegotiatepolicy_binding": [ { "__count":
"#no"} ] }
```

vpnglobal_authenticationpolicy_binding

Binding object showing the authenticationpolicy that can be bound to vpnglobal.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
groupextraction	<Boolean>	Read-write	Bind the Authentication policy to a tertiary chain

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			which will be used only for group extraction. The user will not authenticate against this server, and this will only be called it primary and/or secondary authentication has succeeded.
gotopriorityexpression	<String>	Read-write	Applicable only to advance vpn session policy. An expression or other value specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
policyname	<String>	Read-write	The name of the policy.
priority	<Integer>	Read-write	Integer specifying the policy's priority. The lower the priority number, the higher the policy's priority. Maximum value for default syntax policies is 2147483647 and for classic policies is 64000. Minimum value = 0 Maximum value = 2147483647

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
secondary	<Boolean>	Read-write	Bind the authentication policy as the secondary policy to use in a two-factor configuration. A user must then authenticate not only to a primary authentication server but also to a secondary authentication server. User groups are aggregated across both authentication servers. The user name must be exactly the same on both authentication servers, but the authentication servers can require different passwords.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/vpnglobal_authenticationpolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"vpnglobal_authenticationpolicy_binding":{

"policyname":<String_value>,
```

```
"priority":<Integer_value>,

"secondary":<Boolean_value>,

"groupextraction":<Boolean_value>,

"gotopriorityexpression":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_authenticationpolicy_binding **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_authenticationpolicy_binding? **args=policyname: <String_value> ,secondary: <Boolean_value> ,groupextraction: <Boolean_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_authenticationpolicy_binding **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_authenticationpolicy_binding? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of vpnglobal_authenticationpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_authenticationpolicy_binding? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vpnglobal_authenticationpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnglobal_authenticationpolicy_binding": [ {

"groupextraction":<Boolean_value>,

"gotopriorityexpression":<String_value>,

"policyname":<String_value>,

"priority":<Integer_value>,

"secondary":<Boolean_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_authenticationpolicy_binding? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vpnglobal_authenticationpolicy_binding": [ { "__count": "#no"} ] }
```

vpnglobal_authenticationradiuspolicy_binding

Binding object showing the authenticationradiuspolicy that can be bound to vpnglobal.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
gotopriorityexpression	<String>	Read-write	Applicable only to advance vpn session policy. An expression or other value specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
policyname	<String>	Read-write	The name of the policy.
groupextraction	<Boolean>	Read-write	Bind the Authentication policy

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			to a tertiary chain which will be used only for group extraction. The user will not authenticate against this server, and this will only be called it primary and/or secondary authentication has succeeded.
priority	<Integer>	Read-write	Integer specifying the policy's priority. The lower the priority number, the higher the policy's priority. Maximum value for default syntax policies is 2147483647 and for classic policies is 64000. Minimum value = 0 Maximum value = 2147483647
secondary	<Boolean>	Read-write	Bind the authentication policy as the secondary policy to use in a two-factor configuration. A user must then authenticate not only to a primary authentication server but also to a secondary authentication

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			server. User groups are aggregated across both authentication servers. The user name must be exactly the same on both authentication servers, but the authentication servers can require different passwords.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/vpnglobal_authenticationradiuspolicy_binding
HTTP Method: PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"vpnglobal_authenticationradiuspolicy_binding":{

"policyname":<String_value>,

"priority":<Integer_value>,

"secondary":<Boolean_value>,

"groupextraction":<Boolean_value>,

"gotopriorityexpression":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_authenticationradiuspolicy_binding **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_authenticationradiuspolicy_binding? **args=policyname: <String_value> ,secondary: <Boolean_value> ,groupextraction: <Boolean_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_authenticationradiuspolicy_binding **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_authenticationradiuspolicy_binding? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of vpnglobal_authenticationradiuspolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_authenticationradiuspolicy_binding? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vpnglobal_authenticationradiuspolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnglobal_authenticationradiuspolicy_binding": [ {

"gotopriorityexpression":<String_value>,

"policyname":<String_value>,

"groupextraction":<Boolean_value>,

"priority":<Integer_value>,

"secondary":<Boolean_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_authenticationradiuspolicy_binding?**count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vpnglobal_authenticationradiuspolicy_binding": [ { "__count":
"#no"} ] }
```

vpnglobal_authenticationsamlpolicy_binding

Binding object showing the authenticationsamlpolicy that can be bound to vpnglobal.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
secondary	<Boolean>	Read-write	Bind the authentication policy as the secondary policy to use in a two-factor configuration. A user must then authenticate not only to a primary authentication server but also to a secondary authentication server. User groups are aggregated across both authentication servers. The user name must be exactly the same on both authentication servers, but the authentication servers can require different passwords.
priority	<Integer>	Read-write	Integer specifying the policy's priority. The lower the priority

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			number, the higher the policy's priority. Maximum value for default syntax policies is 2147483647 and for classic policies is 64000. Minimum value = 0 Maximum value = 2147483647
groupextraction	<Boolean>	Read-write	Bind the Authentication policy to a tertiary chain which will be used only for group extraction. The user will not authenticate against this server, and this will only be called it primary and/or secondary authentication has succeeded.
policyname	<String>	Read-write	The name of the policy.
gotopriorityexpression	<String>	Read-write	Applicable only to advance vpn session policy. An expression or other value specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/vpnglobal_authenticationsamlpolicy_binding
HTTP Method: PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"vpnglobal_authenticationsamlpolicy_binding":{

"policyname":<String_value>,

"priority":<Integer_value>,

"secondary":<Boolean_value>,

"groupextraction":<Boolean_value>,

"gotopriorityexpression":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_authenticationsamlpolicy_binding
Query-parameters: args http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_authenticationsamlpolicy_binding? **args=policyname: <String_value> ,secondary: <Boolean_value> ,groupextraction: <Boolean_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_authenticationsamlpolicy_binding **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_authenticationsamlpolicy_binding? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of vpnglobal_authenticationsamlpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_authenticationsamlpolicy_binding? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vpnglobal_authenticationsamlpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnglobal_authenticationsamlpolicy_binding": [ {

"secondary":<Boolean_value>,
```

```
"priority":<Integer_value>,

"groupextraction":<Boolean_value>,

"policyname":<String_value>,

"gotopriorityexpression":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_authenticationsamlpolicy_binding?**count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vpnglobal_authenticationsamlpolicy_binding": [ { "__count": "#no"} ] }
```

vpnglobal_authenticationtacacspolicy_binding

Binding object showing the authenticationtacacspolicy that can be bound to vpnglobal.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
secondary	<Boolean>	Read-write	Bind the authentication policy as the secondary policy to use in a two-factor configuration. A user must then authenticate not only to a primary authentication server but also to a secondary authentication server. User groups are aggregated across both authentication servers. The user name must be exactly the same on both authentication servers, but the authentication servers can require different passwords.
priority	<Integer>	Read-write	Integer specifying the policy's priority. The lower the priority number, the higher the policy's priority. Maximum value for default syntax policies is 2147483647 and for classic policies is 64000. Minimum value = 0

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum value = 2147483647
policyname	<String>	Read-write	The name of the policy.
gotopriorityexpression	<String>	Read-write	Applicable only to advance vpn session policy. An expression or other value specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
groupextraction	<Boolean>	Read-write	Bind the Authentication policy to a tertiary chain which will be used only for group extraction. The user will not authenticate against this server, and this will only be called it primary and/or secondary authentication has succeeded.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET

- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/vpnglobal_authenticationtacacspolicy_binding
HTTP Method: PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"vpnglobal_authenticationtacacspolicy_binding":{

"policyname":<String_value>,

"priority":<Integer_value>,

"secondary":<Boolean_value>,

"groupextraction":<Boolean_value>,

"gotopriorityexpression":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_authenticationtacacspolicy_binding **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_authenticationtacacspolicy_binding? **args=policyname: <String_value> ,secondary: <Boolean_value> ,groupextraction: <Boolean_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_authenticationtacacspolicy_binding **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/

vpnglobal_authenticationtacacspolicy_binding? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of vpnglobal_authenticationtacacspolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ vpnglobal_authenticationtacacspolicy_binding? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vpnglobal_authenticationtacacspolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnglobal_authenticationtacacspolicy_binding": [ {

"secondary":<Boolean_value>,

"priority":<Integer_value>,

"policyname":<String_value>,

"gotopriorityexpression":<String_value>,

"groupextraction":<Boolean_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_authenticationtacacspolicy_binding?**count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vpnglobal_authenticationtacacspolicy_binding": [ { "__count":
"#no"} ] }
```

vpnglobal_binding

Binding object which returns the resources bound to vpnglobal.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
vpnglobal_vpnportaltheme_binding	<vpnglobal_vpnportaltheme_binding[]>	Read-write	vpnportaltheme that can be bound to vpnglobal.
vpnglobal_vpnclientlessaccesspolicy_binding	<vpnglobal_vpnclientlessaccesspolicy_binding[]>	Read-write	vpnclientlessaccesspolicy that can be bound to vpnglobal.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
vpnglobal_authenticationtacacspolicy_binding	<vpnglobal_authenticationtacacspolicy_binding[]>	Read-write	authenticationtacacspolicy that can be bound to vpnglobal.
vpnglobal_appcontroller_binding	<vpnglobal_appcontroller_binding[]>	Read-write	appcontroller that can be bound to vpnglobal.
vpnglobal_authenticationradiuspolicy_binding	<vpnglobal_authenticationradiuspolicy_binding[]>	Read-write	authenticationradiuspolicy that can be bound to vpnglobal.
vpnglobal_vpneula_binding	<vpnglobal_vpneula_binding[]>	Read-write	vpneula that can be bound to vpnglobal.
vpnglobal_vpntrafficpolicy_binding	<vpnglobal_vpntrafficpolicy_binding[]>	Read-write	vpntrafficpolicy that can be bound to vpnglobal.
vpnglobal_authenticationpolicy_binding	<vpnglobal_authenticationpolicy_binding[]>	Read-write	authenticationpolicy that can be bound to vpnglobal.
vpnglobal_authenticationsamlpolicy_binding	<vpnglobal_authenticationsamlpolicy_binding[]>	Read-write	authenticationsamlpolicy that can be bound to vpnglobal.
vpnglobal_sharefileserver_binding	<vpnglobal_sharefileserver_binding[]>	Read-write	sharefileserver that can be bound to vpnglobal.
vpnglobal_auditnslogpolicy_binding	<vpnglobal_auditnslogpolicy_binding[]>	Read-write	auditnslogpolicy that can be bound to vpnglobal.
vpnglobal_intranetip_binding	<vpnglobal_intranetip_binding[]>	Read-write	intranetip that can be bound to vpnglobal.
vpnglobal_authenticationcertpolicy_binding	<vpnglobal_authenticationcertpolicy_binding[]>	Read-write	authenticationcertpolicy that can be bound to vpnglobal.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
vpnglobal_staserver_binding	<vpnglobal_staserver_binding[]>	Read-write	staserver that can be bound to vpnglobal.
vpnglobal_auditsyslogpolicy_binding	<vpnglobal_auditsyslogpolicy_binding[]>	Read-write	auditsyslogpolicy that can be bound to vpnglobal.
vpnglobal_vpnsecureprivateaccessprofile_binding	<vpnglobal_vpnsecureprivateaccessprofile_binding[]>	Read-write	vpnsecureprivateaccessprofile that can be bound to vpnglobal.
vpnglobal_sslcertkey_binding	<vpnglobal_sslcertkey_binding[]>	Read-write	sslcertkey that can be bound to vpnglobal.
vpnglobal_vpnsessionpolicy_binding	<vpnglobal_vpnsessionpolicy_binding[]>	Read-write	vpnsessionpolicy that can be bound to vpnglobal.
vpnglobal_vpnurl_binding	<vpnglobal_vpnurl_binding[]>	Read-write	vpnurl that can be bound to vpnglobal.
vpnglobal_vpnurlpolicy_binding	<vpnglobal_vpnurlpolicy_binding[]>	Read-write	vpnurlpolicy that can be bound to vpnglobal.
vpnglobal_authenticationnegotiatepolicy_binding	<vpnglobal_authenticationnegotiatepolicy_binding[]>	Read-write	authenticationnegotiatepolicy that can be bound to vpnglobal.
vpnglobal_appfwpolicy_binding	<vpnglobal_appfwpolicy_binding[]>	Read-write	appfwpolicy that can be bound to vpnglobal.
vpnglobal_vpnintranetapplication_binding	<vpnglobal_vpnintranetapplication_binding[]>	Read-write	vpnintranetapplication that can be bound to vpnglobal.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
vpnglobal_secureprivateaccessurl_binding	<vpnglobal_secureprivateaccessurl_binding[]>	Read-write	secureprivateaccessurl that can be bound to vpnglobal.
vpnglobal_authenticationldappolicy_binding	<vpnglobal_authenticationldappolicy_binding[]>	Read-write	authenticationldappolicy that can be bound to vpnglobal.
vpnglobal_domain_binding	<vpnglobal_domain_binding[]>	Read-write	domain that can be bound to vpnglobal.
vpnglobal_intranetip6_binding	<vpnglobal_intranetip6_binding[]>	Read-write	intranetip6 that can be bound to vpnglobal.
vpnglobal_authenticationlocalpolicy_binding	<vpnglobal_authenticationlocalpolicy_binding[]>	Read-write	authenticationlocalpolicy that can be bound to vpnglobal.
vpnglobal_vpnnexthopserver_binding	<vpnglobal_vpnnexthopserver_binding[]>	Read-write	vpnnexthopserver that can be bound to vpnglobal.

Operations

(click to see Properties)

- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of

creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vpnglobal_binding": [ {

"vpnglobal_appcontroller_binding":<vpnglobal_appcontroller_binding[]_value
>,

"vpnglobal_vpnurl_binding":<vpnglobal_vpnurl_binding[]_value>,

"vpnglobal_intranetip6_binding":<vpnglobal_intranetip6_binding[]_value>,
```

```
"vpnglobal_authenticationnegotiatepolicy_binding":<vpnglobal_authenticatio
nnegotiatepolicy_binding[]_value>,

"vpnglobal_sslcertkey_binding":<vpnglobal_sslcertkey_binding[]_value>,

"vpnglobal_vpnclientlessaccesspolicy_binding":<vpnglobal_vpnclientlessacce
sspolicy_binding[]_value>,

"vpnglobal_sharefileserver_binding":<vpnglobal_sharefileserver_binding[]_v
alue>,

"vpnglobal_vpntrafficpolicy_binding":<vpnglobal_vpntrafficpolicy_binding[]
_value>,

"vpnglobal_authenticationradiuspolicy_binding":<vpnglobal_authenticationra
diuspolicy_binding[]_value>,

"vpnglobal_vpnintranetapplication_binding":<vpnglobal_vpnintranetapplicati
on_binding[]_value>,

"vpnglobal_authenticationsamlpolicy_binding":<vpnglobal_authenticationsaml
policy_binding[]_value>,

"vpnglobal_secureprivateaccessurl_binding":<vpnglobal_secureprivateaccessu
rl_binding[]_value>,

"vpnglobal_authenticationpolicy_binding":<vpnglobal_authenticationpolicy_b
inding[]_value>,

"vpnglobal_auditnslogpolicy_binding":<vpnglobal_auditnslogpolicy_binding[]
_value>,

"vpnglobal_domain_binding":<vpnglobal_domain_binding[]_value>,

"vpnglobal_vpnsessionpolicy_binding":<vpnglobal_vpnsessionpolicy_binding[]
_value>,

"vpnglobal_vpnnexthopserver_binding":<vpnglobal_vpnnexthopserver_binding[]
_value>,

"vpnglobal_staserver_binding":<vpnglobal_staserver_binding[]_value>,

"vpnglobal_vpneula_binding":<vpnglobal_vpneula_binding[]_value>,
```

```
"vpnglobal_appfwpolicy_binding":<vpnglobal_appfwpolicy_binding[]_value>,

"vpnglobal_vpnportaltheme_binding":<vpnglobal_vpnportaltheme_binding[]_val
ue>,

"vpnglobal_vpnurlpolicy_binding":<vpnglobal_vpnurlpolicy_binding[]_value>,

"vpnglobal_authenticationtacacspolicy_binding":<vpnglobal_authenticationta
cacspolicy_binding[]_value>,

"vpnglobal_vpnsecureprivateaccessprofile_binding":<vpnglobal_vpnsecurepriv
ateaccessprofile_binding[]_value>,

"vpnglobal_authenticationldappolicy_binding":<vpnglobal_authenticationldap
policy_binding[]_value>,

"vpnglobal_authenticationcertpolicy_binding":<vpnglobal_authenticationcert
policy_binding[]_value>,

"vpnglobal_authenticationlocalpolicy_binding":<vpnglobal_authenticationloc
alpolicy_binding[]_value>,

"vpnglobal_auditsyslogpolicy_binding":<vpnglobal_auditsyslogpolicy_binding
[]_value>,

"vpnglobal_intranetip_binding":<vpnglobal_intranetip_binding[]_value>

}]}
```

vpnglobal_domain_binding

Binding object showing the domain that can be bound to vpnglobal.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
intranetdomain	<String>	Read-write	The conflicting intranet domain name.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
gotopriorityexpression	<String>	Read-write	Applicable only to advance vpn session policy. An expression or other value specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/vpnglobal_domain_binding

HTTP Method: PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"vpnglobal_domain_binding":{

"intranetdomain":<String_value>,

"gotopriorityexpression":<String_value>

}}
```

Response:

HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_domain_binding

Query-parameters:

args

http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_domain_binding? **args=intranetdomain:<String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_domain_binding

Query-parameters:

filter

http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_domain_binding? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of vpnglobal_domain_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination

http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_domain_binding? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vpnglobal_domain_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnglobal_domain_binding": [ {

"intranetdomain":<String_value>,

"gotopriorityexpression":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_domain_binding? **count=yes**

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vpnglobal_domain_binding": [ { "__count": "#no"} ] }
```

vpnglobal_intranetip6_binding

Binding object showing the intranetip6 that can be bound to vpnglobal.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
intranetip6	<String>	Read-write	The intranet ip address or range.
gotopriorityexpression	<String>	Read-write	Applicable only to advance vpn session policy. An expression or other value specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
numaddr	<Integer>	Read-write	The intranet ip address or range's netmask.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/vpnglobal_intranetip6_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"vpnglobal_intranetip6_binding":{

"intranetip6":<String_value>,

"numaddr":<Integer_value>,

"gotopriorityexpression":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_intranetip6_binding **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_intranetip6_binding? **args=intranetip6: <String_value> ,numaddr: <Integer_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_intranetip6_binding **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_intranetip6_binding?**filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of vpnglobal_intranetip6_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_intranetip6_binding?**pagesize=#no;pageno=#no**

Use this query-parameter to get the vpnglobal_intranetip6_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnglobal_intranetip6_binding": [ {

"intranetip6":<String_value>,

"gotopriorityexpression":<String_value>,

"numaddr":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_intranetip6_binding? **count=yes**
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vpnglobal_intranetip6_binding": [ { "__count": "#no"} ] }
```

vpnglobal_intranetip_binding

Binding object showing the intranetip that can be bound to vpnglobal.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
gotopriorityexpression	<String>	Read-write	Applicable only to advance vpn session policy. An expression or other value specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
netmask	<String>	Read-write	The intranet ip address or range's netmask.
intranetip	<String>	Read-write	The intranet ip address or range.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/vpnglobal_intranetip_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"vpnglobal_intranetip_binding":{

"intranetip":<String_value>,

"netmask":<String_value>,

"gotopriorityexpression":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_intranetip_binding **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_intranetip_binding? **args=intranetip: <String_value> ,netmask: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_intranetip_binding **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_intranetip_binding?**filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of vpnglobal_intranetip_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_intranetip_binding?**pagesize=#no;pageno=#no**

Use this query-parameter to get the vpnglobal_intranetip_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnglobal_intranetip_binding": [ {

"gotopriorityexpression":<String_value>,

"netmask":<String_value>,
```

```
"intranetip":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_intranetip_binding? **count=yes**
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vpnglobal_intranetip_binding": [ { "__count": "#no"} ] }
```

vpnglobal_secureprivateaccessurl_binding

Binding object showing the secureprivateaccessurl that can be bound to vpnglobal.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
gotopriorityexpression	<String>	Read-write	Applicable only to advance vpn session policy. An expression or other value

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
secureprivateaccessurl	<String>	Read-write	Configured Secure Private Access URL.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/vpnglobal_secureprivateaccessurl_binding

HTTP Method: PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"vpnglobal_secureprivateaccessurl_binding":{

"secureprivateaccessurl":<String_value>,

"gotopriorityexpression":<String_value>

}}
```

Response:

HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_secureprivateaccessurl_binding

Query-parameters:

args

http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_secureprivateaccessurl_binding?**args=secureprivateaccessurl: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_secureprivateaccessurl_binding

Query-parameters:

filter

http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_secureprivateaccessurl_binding?**filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of vpnglobal_secureprivateaccessurl_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination

http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_secureprivateaccessurl_binding?**pagesize=#no;pageno=#no**

Use this query-parameter to get the vpnglobal_secureprivateaccessurl_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnglobal_secureprivateaccessurl_binding": [ {

"gotopriorityexpression":<String_value>,

"secureprivateaccessurl":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_secureprivateaccessurl_binding?**count=yes**

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vpnglobal_secureprivateaccessurl_binding": [ { "__count": "#no"} ] }
```

vpnglobal_sharefileserver_binding

Binding object showing the sharefileserver that can be bound to vpnglobal.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
sharefile	<String>	Read-write	Configured Sharefile server, in the format IP:PORT / FQDN:PORT.
gotopriorityexpression	<String>	Read-write	Applicable only to advance vpn session policy. An expression or other value specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/vpnglobal_sharefileserver_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"vpnglobal_sharefileserver_binding":{

"sharefile":<String_value>,

"gotopriorityexpression":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_sharefileserver_binding **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_sharefileserver_binding? **args=sharefile: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_sharefileserver_binding **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/

vpnglobal_sharefileserver_binding? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of vpnglobal_sharefileserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_sharefileserver_binding? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vpnglobal_sharefileserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnglobal_sharefileserver_binding": [ {

"sharefile":<String_value>,

"gotopriorityexpression":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_sharefileserver_binding? **count=yes**
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vpnglobal_sharefileserver_binding": [ { "__count": "#no"} ] }
```

vpnglobal_sslcertkey_binding

Binding object showing the sslcertkey that can be bound to vpnglobal.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
gotopriorityexpression	<String>	Read-write	Applicable only to advance vpn session policy. An expression or other value specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
certkeyname	<String>	Read-write	SSL certkey to use in signing tokens. Only RSA cert key is allowed.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ocspcheck	<String>	Read-write	The state of the OCSP check parameter (Mandatory/ Optional). Possible values = Mandatory, Optional
crlcheck	<String>	Read-write	The state of the CRL check parameter (Mandatory/ Optional). Possible values = Mandatory, Optional
userdataencryptionkey	<String>	Read-write	Certificate to be used for encrypting user data like KB Question and Answers, Alternate Email Address, etc.
cacert	<String>	Read-write	The name of the CA certificate binding.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/vpnglobal_sslcertkey_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"vpnglobal_sslcertkey_binding":{

"gotopriorityexpression":<String_value>,
```

```
"certkeyname":<String_value>,

"userdataencryptionkey":<String_value>,

"cacert":<String_value>,

"crlcheck":<String_value>,

"ocspcheck":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_sslcertkey_binding **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_sslcertkey_binding? **args=certkeyname: <String_value> ,userdataencryptionkey: <String_value> ,cacert: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_sslcertkey_binding **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_sslcertkey_binding? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of vpnglobal_sslcertkey_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_sslcertkey_binding? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vpnglobal_sslcertkey_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnglobal_sslcertkey_binding": [ {

"gotopriorityexpression":<String_value>,

"certkeyname":<String_value>,

"ocspcheck":<String_value>,

"crlcheck":<String_value>,

"userdataencryptionkey":<String_value>,

"cacert":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_sslcertkey_binding? **count=yes**
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vpnglobal_sslcertkey_binding": [ { "__count": "#no"} ] }
```

vpnglobal_staserver_binding

Binding object showing the staserver that can be bound to vpnglobal.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
staaddresstype	<String>	Read-write	Type of the STA server address(ipv4/v6). Possible values = IPV4, IPV6
gotopriorityexpression	<String>	Read-write	Applicable only to advance vpn session policy. An expression or other value specifying the priority of the next policy which will get evaluated if the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			current policy rule evaluates to TRUE.
staserver	<String>	Read-write	Configured Secure Ticketing Authority (STA) server.
staauthid	<String>	Read-only	Authority ID of the STA Server. Authority ID is used to match incoming STA Tickets in the SOCKS/CGP protocol with the right STA Server.
stastate	<String>	Read-only	State of the STA Server. If Authority ID is set then STA Server is UP else DOWN. Possible values = UP, DOWN
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/vpnglobal_staserver_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"vpnglobal_staserver_binding":{

"staserver":<String_value>,

"staaddresstype":<String_value>,

"gotopriorityexpression":<String_value>
```

```
}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_staserver_binding **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_staserver_binding? **args=staserver: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_staserver_binding **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_staserver_binding? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of vpnglobal_staserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_staserver_binding? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vpnglobal_staserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnglobal_staserver_binding": [ {

"staaddresstype":<String_value>,

"gotopriorityexpression":<String_value>,

"staserver":<String_value>,

"staauthid":<String_value>,

"stastate":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_staserver_binding? **count=yes**
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vpnglobal_staserver_binding": [ { "__count": "#no"} ] }
```

vpnglobal_vpnclientlessaccesspolicy_binding

Binding object showing the vpnclientlessaccesspolicy that can be bound to vpnglobal.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
feature	<String>	Read-write	The feature to be checked while applying this config.
gotopriorityexpression	<String>	Read-write	Applicable only to advance vpn session policy. An expression or other value specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
globalbindtype	<String>	Read-write	. Possible values = SYSTEM_GLOBAL, VPN_GLOBAL, RNAT_GLOBAL, APPFW_GLOBAL, TM_GLOBAL
policyname	<String>	Read-write	The name of the policy.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
groupextraction	<Boolean>	Read-write	Bind the Authentication policy to a tertiary chain which will be used only for group extraction. The user will not authenticate against this server, and this will only be called it primary and/or secondary authentication has succeeded.
type	<String>	Read-write	Bindpoint to which the policy is bound. Possible values = REQ_OVERRIDE, REQ_DEFAULT, RES_OVERRIDE, RES_DEFAULT
builtin	<String[]>	Read-write	Indicates that a variable is a built-in (SYSTEM INTERNAL) type. Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL
secondary	<Boolean>	Read-write	Bind the authentication policy as the secondary policy to use in a two-factor configuration. A user must then

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			authenticate not only to a primary authentication server but also to a secondary authentication server. User groups are aggregated across both authentication servers. The user name must be exactly the same on both authentication servers, but the authentication servers can require different passwords.
priority	<Integer>	Read-write	Integer specifying the policy's priority. The lower the priority number, the higher the policy's priority. Maximum value for default syntax policies is 2147483647 and for classic policies is 64000. Minimum value = 0 Maximum value = 2147483647
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD

- DELETE
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/vpnglobal_vpnclientlessaccesspolicy_binding
HTTP Method: PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"vpnglobal_vpnclientlessaccesspolicy_binding":{

"policyname":<String_value>,

"priority":<Integer_value>,

"secondary":<Boolean_value>,

"groupextraction":<Boolean_value>,

"gotopriorityexpression":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_vpnclientlessaccesspolicy_binding **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_vpnclientlessaccesspolicy_binding? **args=policyname: <String_value> ,secondary: <Boolean_value> ,groupextraction: <Boolean_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_vpnclientlessaccesspolicy_binding **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/

vpnglobal_vpnclientlessaccesspolicy_binding? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of vpnglobal_vpnclientlessaccesspolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ vpnglobal_vpnclientlessaccesspolicy_binding? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vpnglobal_vpnclientlessaccesspolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnglobal_vpnclientlessaccesspolicy_binding": [ {

"feature":<String_value>,

"gotopriorityexpression":<String_value>,

"globalbindtype":<String_value>,

"policyname":<String_value>,

"groupextraction":<Boolean_value>,

"type":<String_value>,
```

```
"builtin":<String[]_value>,

"secondary":<Boolean_value>,

"priority":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_vpnclientlessaccesspolicy_binding?**count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vpnglobal_vpnclientlessaccesspolicy_binding": [ { "__count": "#no"} ] }
```

vpnglobal_vpneula_binding

Binding object showing the vpneula that can be bound to vpnglobal.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
gotopriorityexpression	<String>	Read-write	Applicable only to advance vpn session policy. An expression or other value specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
eula	<String>	Read-write	Name of the EULA bound to vpnglobal.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/vpnglobal_vpneula_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"vpnglobal_vpneula_binding":{

"gotopriorityexpression":<String_value>,

"eula":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_vpneula_binding **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_vpneula_binding? **args=eula: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_vpneula_binding **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_vpneula_binding?**filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of vpnglobal_vpneula_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_vpneula_binding?**pagesize=#no;pageno=#no**

Use this query-parameter to get the vpnglobal_vpneula_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnglobal_vpneula_binding": [ {

"gotopriorityexpression":<String_value>,

"eula":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_vpneula_binding? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vpnglobal_vpneula_binding": [ { "__count": "#no"} ] }
```

vpnglobal_vpnintranetapplication_binding

Binding object showing the vpnintranetapplication that can be bound to vpnglobal.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
gotopriorityexpression	<String>	Read-write	Applicable only to advance vpn session policy. An expression or other value specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
intranetapplication	<String>	Read-write	The intranet vpn application.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/vpnglobal_vpnintranetapplication_binding

HTTP Method: PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"vpnglobal_vpnintranetapplication_binding":{

"intranetapplication":<String_value>,

"gotopriorityexpression":<String_value>

}}
```

Response:

HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_vpnintranetapplication_binding

Query-parameters:

args

http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_vpnintranetapplication_binding?**args=intranetapplication: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_vpnintranetapplication_binding

Query-parameters:

filter

http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_vpnintranetapplication_binding?**filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of vpnglobal_vpnintranetapplication_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination

http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_vpnintranetapplication_binding?**pagesize=#no;pageno=#no**

Use this query-parameter to get the vpnglobal_vpnintranetapplication_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnglobal_vpnintranetapplication_binding": [ {

"gotopriorityexpression":<String_value>,

"intranetapplication":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_vpnintranetapplication_binding?**count=yes**

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vpnglobal_vpnintranetapplication_binding": [ { "__count": "#no"} ] }
```

vpnglobal_vpnnexthopserver_binding

Binding object showing the vpnnexthopserver that can be bound to vpnglobal.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
gotopriorityexpression	<String>	Read-write	Applicable only to advance vpn session policy. An expression or other value specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
nexthopserver	<String>	Read-write	The name of the next hop server bound to vpn global.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/vpnglobal_vpnnexthopserver_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"vpnglobal_vpnnexthopserver_binding":{

"nexthopserver":<String_value>,

"gotopriorityexpression":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_vpnnexthopserver_binding **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_vpnnexthopserver_binding? **args=nexthopserver: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_vpnnexthopserver_binding **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/

vpnglobal_vpnnexthopserver_binding? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of vpnglobal_vpnnexthopserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_vpnnexthopserver_binding? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vpnglobal_vpnnexthopserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnglobal_vpnnexthopserver_binding": [ {

"gotopriorityexpression":<String_value>,

"nexthopserver":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_vpnnexthopserver_binding? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vpnglobal_vpnnexthopserver_binding": [ { "__count": "#no"} ] }
```

vpnglobal_vpnportaltheme_binding

Binding object showing the vpnportaltheme that can be bound to vpnglobal.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
portaltheme	<String>	Read-write	Name of the portal theme bound to vpnglobal.
gotopriorityexpression	<String>	Read-write	Applicable only to advance vpn session policy. An expression or other value specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/vpnglobal_vpnportaltheme_binding

HTTP Method: PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"vpnglobal_vpnportaltheme_binding":{

"gotopriorityexpression":<String_value>,

"portaltheme":<String_value>

}}
```

Response:

HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_vpnportaltheme_binding

Query-parameters:

args

http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_vpnportaltheme_binding?
args=portaltheme: <String_value>

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_vpnportaltheme_binding

Query-parameters:

filter

http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_vpnportaltheme_binding? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of vpnglobal_vpnportaltheme_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination

http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_vpnportaltheme_binding? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vpnglobal_vpnportaltheme_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnglobal_vpnportaltheme_binding": [ {

"portaltheme":<String_value>,

"gotopriorityexpression":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_vpnportaltheme_binding?**count=yes**

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vpnglobal_vpnportaltheme_binding": [ { "__count": "#no"} ] }
```

vpnglobal_vpnsecureprivateaccessprofile_binding

Binding object showing the vpnsecureprivateaccessprofile that can be bound to vpnglobal.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
secureprivateaccessprofile	<String>	Read-write	The name of the Secure Private Access Profile bound to vpn global. Minimum length = 1 Maximum length = 31
gotopriorityexpression	<String>	Read-write	Applicable only to advance vpn session policy. An expression or other value specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/vpnglobal_vpnsecureprivateaccessprofile_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"vpnglobal_vpnsecureprivateaccessprofile_binding":{

"gotopriorityexpression":<String_value>,
```

```
"secureprivateaccessprofile":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/ vpnglobal_vpnsecureprivateaccessprofile_binding **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_vpnsecureprivateaccessprofile_binding? **args=secureprivateaccessprofile: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/ vpnglobal_vpnsecureprivateaccessprofile_binding **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_vpnsecureprivateaccessprofile_binding? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of vpnglobal_vpnsecureprivateaccessprofile_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ vpnglobal_vpnsecureprivateaccessprofile_binding? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vpnglobal_vpnsecureprivateaccessprofile_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnglobal_vpnsecureprivateaccessprofile_binding": [ {

"secureprivateaccessprofile":<String_value>,

"gotopriorityexpression":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/ vpnglobal_vpnsecureprivateaccessprofile_binding? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vpnglobal_vpnsecureprivateaccessprofile_binding": [ { "__count":
"#no"} ] }
```

vpnglobal_vpnsessionpolicy_binding

Binding object showing the vpnsessionpolicy that can be bound to vpnglobal.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
secondary	<Boolean>	Read-write	Bind the authentication policy as the secondary policy to use in a two-factor configuration. A user must then authenticate not only to a primary authentication server but also to a secondary authentication server. User groups are aggregated across both authentication servers. The user name must be exactly the same on both authentication servers, but the authentication servers can require different passwords.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
priority	<Integer>	Read-write	Integer specifying the policy's priority. The lower the priority number, the higher the policy's priority. Maximum value for default syntax policies is 2147483647 and for classic policies is 64000. Minimum value = 0 Maximum value = 2147483647
feature	<String>	Read-write	The feature to be checked while applying this config.
gotopriorityexpression	<String>	Read-write	Applicable only to advance vpn session policy. An expression or other value specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
policyname	<String>	Read-write	The name of the policy.
groupextraction	<Boolean>	Read-write	Bind the Authentication policy to a tertiary chain which will be used only for group extraction. The user will not authenticate

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			against this server, and this will only be called it primary and/or secondary authentication has succeeded.
builtin	<String[]>	Read-write	Indicates that a variable is a built-in (SYSTEM INTERNAL) type. Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/vpnglobal_vpnsessionpolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"vpnglobal_vpnsessionpolicy_binding":{

"policyname":<String_value>,

"priority":<Integer_value>,

"secondary":<Boolean_value>,

"groupextraction":<Boolean_value>,

"gotopriorityexpression":<String_value>
```

```
}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_vpnsessionpolicy_binding **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_vpnsessionpolicy_binding? **args=policyname: <String_value> ,secondary: <Boolean_value> ,groupextraction: <Boolean_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_vpnsessionpolicy_binding **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_vpnsessionpolicy_binding? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of vpnglobal_vpnsessionpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_vpnsessionpolicy_binding? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vpnglobal_vpnsessionpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnglobal_vpnsessionpolicy_binding": [ {

"secondary":<Boolean_value>,

"priority":<Integer_value>,

"feature":<String_value>,

"gotopriorityexpression":<String_value>,

"policyname":<String_value>,

"groupextraction":<Boolean_value>,

"builtin":<String[]_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_vpnsessionpolicy_binding?**count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vpnglobal_vpnsessionpolicy_binding": [ { "__count": "#no"} ] }
```

vpnglobal_vpntrafficpolicy_binding

Binding object showing the vpntrafficpolicy that can be bound to vpnglobal.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
secondary	<Boolean>	Read-write	Bind the authentication policy as the secondary policy to use in a two-factor configuration. A user must then authenticate not only to a primary authentication server but also to a secondary authentication server. User groups are aggregated across both authentication servers. The user name must be exactly the same on

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			both authentication servers, but the authentication servers can require different passwords.
priority	<Integer>	Read-write	Integer specifying the policy's priority. The lower the priority number, the higher the policy's priority. Maximum value for default syntax policies is 2147483647 and for classic policies is 64000. Minimum value = 0 Maximum value = 2147483647
policyname	<String>	Read-write	The name of the policy.
gotopriorityexpression	<String>	Read-write	Applicable only to advance vpn session policy. An expression or other value specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
groupextraction	<Boolean>	Read-write	Bind the Authentication policy to a tertiary chain which will be used only for group

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			extraction. The user will not authenticate against this server, and this will only be called it primary and/or secondary authentication has succeeded.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/vpnglobal_vpntrafficpolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"vpnglobal_vpntrafficpolicy_binding":{

"policyname":<String_value>,

"priority":<Integer_value>,

"secondary":<Boolean_value>,

"groupextraction":<Boolean_value>,

"gotopriorityexpression":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_vpntrafficpolicy_binding **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_vpntrafficpolicy_binding? **args=policyname: <String_value> ,secondary: <Boolean_value> ,groupextraction: <Boolean_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_vpntrafficpolicy_binding **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_vpntrafficpolicy_binding? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of vpnglobal_vpntrafficpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_vpntrafficpolicy_binding? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vpnglobal_vpntrafficpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnglobal_vpntrafficpolicy_binding": [ {

"secondary":<Boolean_value>,

"priority":<Integer_value>,

"policyname":<String_value>,

"gotopriorityexpression":<String_value>,

"groupextraction":<Boolean_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_vpntrafficpolicy_binding? **count=yes**
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vpnglobal_vpntrafficpolicy_binding": [ { "__count": "#no"} ] }
```

vpnglobal_vpnurl_binding

Binding object showing the vpnurl that can be bound to vpnglobal.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
gotopriorityexpression	<String>	Read-write	Applicable only to advance vpn session policy. An expression or other value specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
urlname	<String>	Read-write	The intranet url.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/vpnglobal_vpnurl_binding

HTTP Method: PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"vpnglobal_vpnurl_binding":{

"urlname":<String_value>,

"gotopriorityexpression":<String_value>

}}
```

Response:

HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_vpnurl_binding

Query-parameters:

args

http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_vpnurl_binding? **args=urlname: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_vpnurl_binding

Query-parameters:

filter

http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_vpnurl_binding? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of vpnglobal_vpnurl_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination

http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_vpnurl_binding? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vpnglobal_vpnurl_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnglobal_vpnurl_binding": [ {

"gotopriorityexpression":<String_value>,

"urlname":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_vpnurl_binding? **count=yes**

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vpnglobal_vpnurl_binding": [ { "__count": "#no"} ] }
```

vpnglobal_vpnurlpolicy_binding

Binding object showing the vpnurlpolicy that can be bound to vpnglobal.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
builtin	<String[]>	Read-write	Indicates that a variable is a built-in (SYSTEM INTERNAL) type. Possible values = MODIFIABLE, DELETABLE,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			IMMUTABLE, PARTITION_ALL
groupextraction	<Boolean>	Read-write	Bind the Authentication policy to a tertiary chain which will be used only for group extraction. The user will not authenticate against this server, and this will only be called it primary and/or secondary authentication has succeeded.
policyname	<String>	Read-write	The name of the policy.
gotopriorityexpression	<String>	Read-write	Applicable only to advance vpn session policy. An expression or other value specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.
priority	<Integer>	Read-write	Integer specifying the policy's priority. The lower the priority number, the higher the policy's priority. Maximum value for default syntax policies is 2147483647 and for

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			classic policies is 64000. Minimum value = 0 Maximum value = 2147483647
secondary	<Boolean>	Read-write	Bind the authentication policy as the secondary policy to use in a two-factor configuration. A user must then authenticate not only to a primary authentication server but also to a secondary authentication server. User groups are aggregated across both authentication servers. The user name must be exactly the same on both authentication servers, but the authentication servers can require different passwords.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE

- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/vpnglobal_vpnurlpolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"vpnglobal_vpnurlpolicy_binding":{

"policyname":<String_value>,

"priority":<Integer_value>,

"secondary":<Boolean_value>,

"groupextraction":<Boolean_value>,

"gotopriorityexpression":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_vpnurlpolicy_binding **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_vpnurlpolicy_binding? **args=policyname: <String_value> ,secondary: <Boolean_value> ,groupextraction: <Boolean_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_vpnurlpolicy_binding **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_vpnurlpolicy_binding?**filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of vpnglobal_vpnurlpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_vpnurlpolicy_binding?**pagesize=#no;pageno=#no**

Use this query-parameter to get the vpnglobal_vpnurlpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnglobal_vpnurlpolicy_binding": [ {

"builtin":<String[]_value>,

"groupextraction":<Boolean_value>,

"policyname":<String_value>,

"gotopriorityexpression":<String_value>,

"priority":<Integer_value>,
```

```
"secondary":<Boolean_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnglobal_vpnurlpolicy_binding? **count=yes**
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vpnglobal_vpnurlpolicy_binding": [ { "__count": "#no"} ] }
```

vpnicaconnection

Configuration for active ica connections resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
username	<String>	Read-write	User name for which ica connections needs to be terminated.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum length = 1
transproto	<String>	Read-write	Transport type for the existing Existing ICA conenction. Possible values = TCP, UDP
nodeid	<Integer>	Read-write	Unique number that identifies the cluster node. Minimum value = 0 Maximum value = 31
all	<Boolean>	Read-write	Terminate all active icaconnections.
tenantname	<String>	Read-write	Tenant name for which ica connections needs to be terminated. Minimum length = 1
productname	<String>	Read-write	Product name for which ica connections needs to be terminated. Minimum length = 1
domain	<String>	Read-only	The domain name.
srcip	<String>	Read-only	The client IP address.
srcport	<Integer>	Read-only	The client port. Range 1 - 65535 * in CLI is represented as

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			65535 in NITRO API
destip	<String>	Read-only	The CPS server IP address.
destport	<Integer>	Read-only	The CPS server port. Range 1 - 65535 * in CLI is represented as 65535 in NITRO API
peid	<Integer>	Read-only	Core id of the session owner.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET (ALL)
- COUNT
- KILL

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

KILL

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnicaconnection? **action=kill HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"vpnicaconnection":{

"username":<String_value>,

"transproto":<String_value>,

"all":<Boolean_value>,

"tenantname":<String_value>,

"productname":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnicaconnection **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/vpnicaconnection? **args=username: <String_value> ,transproto: <String_value> ,nodeid: <Integer_value>**

Use this query-parameter to get vpnicaconnection resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/config/vpnicaconnection? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/vpnicaconnection? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of vpnicaconnection resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/vpnicaconnection? **view=summary**

Use this query-parameter to get the summary output of vpnicaconnection resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/vpnicaconnection? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vpnicaconnection resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vpnicaconnection": [ {

username:<String_value>,transproto:<String_value>,nodeid:<Integer_value>"d
omain":<String_value>,

"srcip":<String_value>,

"srcport":<Integer_value>,

"destip":<String_value>,

"destport":<Integer_value>,

"peid":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnicaconnection? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vpnicaconnection": [ { "__count": "#no"} ] }
```

vpnicadtlsconnection

Configuration for active ica connections resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
username	<String>	Read-write	User name for which to display connections. Minimum length = 1
nodeid	<Integer>	Read-write	Unique number that identifies the cluster node. Minimum value = 0 Maximum value = 31
domain	<String>	Read-only	The domain name.
srcip	<String>	Read-only	The client IP address.
srcport	<Integer>	Read-only	The client port. Range 1 - 65535

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			* in CLI is represented as 65535 in NITRO API
destip	<String>	Read-only	The CPS server IP address.
destport	<Integer>	Read-only	The CPS server port. Range 1 - 65535 * in CLI is represented as 65535 in NITRO API
channelnumber	<Integer>	Read-only	The channel number.
peid	<Integer>	Read-only	Core id of the session owner.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnicadtlsconnection **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/vpnicadtlsconnection? **args=username: <String_value> ,nodeid: <Integer_value>**

Use this query-parameter to get vpnicadtlsconnection resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/config/vpnicadtlsconnection? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/vpnicadtlsconnection? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of vpnicadtlsconnection resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/vpnicadtlsconnection? **view=summary**

Use this query-parameter to get the summary output of vpnicadtlsconnection resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/vpnicadtlsconnection? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vpnicadtlsconnection resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vpnicadtlsconnection": [ {

username:<String_value>,nodeid:<Integer_value>"domain":<String_value>,

"srcip":<String_value>,

"srcport":<Integer_value>,

"destip":<String_value>,

"destport":<Integer_value>,

"channelnumber":<Integer_value>,

"peid":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnicadtlsconnection? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vpnicadtlsconnection": [ { "__count": "#no"} ] }
```

vpnintranetapplication

Configuration for SSLVPN intranet application resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
intranetapplication	<String>	Read-write	Name of the intranet application. Minimum length = 1 Maximum length = 31

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
protocol	<String>	Read-write	Protocol used by the intranet application. If protocol is set to BOTH, TCP and UDP traffic is allowed. Possible values = TCP, UDP, ANY
destip	<String>	Read-write	Destination IP address, IP range, or host name of the intranet application. This address is the server IP address. Minimum length = 1
netmask	<String>	Read-write	Destination subnet mask for the intranet application.
iprange	<String>	Read-write	If you have multiple servers in your network, such as web, email, and file shares, configure an intranet application that includes the IP range for all the network applications. This allows users to access all the intranet applications contained in the IP address range. Minimum length = 1
hostname	<String>	Read-write	Name of the host for which to configure interception. The

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			names are resolved during interception when users log on with the Citrix Gateway Plug-in. Minimum length = 1
clientapplication	<String[]>	Read-write	Names of the client applications, such as PuTTY and Xshell. Minimum length = 1
spoofiip	<String>	Read-write	IP address that the intranet application will use to route the connection through the virtual adapter. Default value: ON Possible values = ON, OFF
destport	<String>	Read-write	Destination TCP or UDP port number for the intranet application. Use a hyphen to specify a range of port numbers, for example 90-95. Minimum length = 1
interception	<String>	Read-write	Interception mode for the intranet application or resource. Correct value depends on the type of client software used to make connections. If the interception

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			mode is set to TRANSPARENT, users connect with the Citrix Gateway Plug-in for Windows. With the PROXY setting, users connect with the Citrix Gateway Plug-in for Java. Possible values = PROXY, TRANSPARENT
srcip	<String>	Read-write	Source IP address. Required if interception mode is set to PROXY. Default is the loopback address, 127.0.0.1. Minimum length = 1
srcport	<Integer>	Read-write	Source port for the application for which the Citrix Gateway virtual server proxies the traffic. If users are connecting from a device that uses the Citrix Gateway Plug-in for Java, applications must be configured manually by using the source IP address and TCP port values specified in the intranet application profile. If a port value is not

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			set, the destination port value is used. Minimum value = 1
ipaddress	<String>	Read-only	The IP address for the application. This address is the real application server IP address.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnintranetapplication **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"vpnintranetapplication":{

<b>"intranetapplication":<String_value>,

</b>"protocol":<String_value>,

"destip":<String_value>,

"netmask":<String_value>,

"iprange":<String_value>,

"hostname":<String_value>,

"clientapplication":<String[]_value>,

"spoofiip":<String_value>,

"destport":<String_value>,

"interception":<String_value>,
```

```
"srcip":<String_value>,

"srcport":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnintranetapplication/ intranetapplication_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnintranetapplication **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/vpnintranetapplication? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/vpnintranetapplication? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of vpnintranetapplication resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/vpnintranetapplication? **view=summary**

Use this query-parameter to get the summary output of vpnintranetapplication resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/vpnintranetapplication? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vpnintranetapplication resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vpnintranetapplication": [ {

"intranetapplication":<String_value>,

"protocol":<String_value>,

"destip":<String_value>,

"netmask":<String_value>,

"ipaddress":<String_value>,

"hostname":<String_value>,

"destport":<String_value>,

"clientapplication":<String[]_value>,

"spoofiip":<String_value>,
```

```
"interception":<String_value>,

"srcip":<String_value>,

"srcport":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnintranetapplication/ intranetapplication_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/vpnintranetapplication/ intranetapplication_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/vpnintranetapplication/ intranetapplication_value<String> ? **view=summary**

Use this query-parameter to get the summary output of vpnintranetapplication resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnintranetapplication": [ {

"intranetapplication":<String_value>,

"protocol":<String_value>,

"destip":<String_value>,

"netmask":<String_value>,

"ipaddress":<String_value>,

"hostname":<String_value>,

"destport":<String_value>,

"clientapplication":<String[]_value>,

"spoofiip":<String_value>,

"interception":<String_value>,

"srcip":<String_value>,

"srcport":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnintranetapplication? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vpnintranetapplication": [ { "__count": "#no"} ] }
```

vpnnexthopserver

Configuration for Next Hop Server resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the Citrix Gateway appliance in the first DMZ. Minimum length = 1 Maximum length = 32
nexthopip	<String>	Read-write	IP address of the Citrix Gateway proxy in the second DMZ.
nexthopfqdn	<String>	Read-write	FQDN of the Citrix Gateway proxy in the second DMZ. Minimum length = 1
resaddresstype	<String>	Read-write	Address Type (IPV4/IPv6) of DNS name

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			of nextHopServer FQDN. Minimum length = 1 Possible values = IPV4, IPV6
nexthopport	<Integer>	Read-write	Port number of the Citrix Gateway proxy in the second DMZ. Minimum value = 1 Maximum value = 65535
secure	<String>	Read-write	Use of a secure port, such as 443, for the double-hop configuration. Default value: OFF Possible values = ON, OFF
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnnexthopserver **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"vpnnexthopserver":{

<b>"name":<String_value>,

</b>"nexthopip":<String_value>,

"nexthopfqdn":<String_value>,
```

```
"resaddresstype":<String_value>,

<b>"nexthopport":<Integer_value>,

</b>"secure":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnnexthopserver/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnnexthopserver **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/vpnnexthopserver? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/vpnnexthopserver? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of vpnnexthopserver resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/vpnnexthopserver? **view=summary**

Use this query-parameter to get the summary output of vpnnexthopserver resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/vpnnexthopserver? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vpnnexthopserver resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vpnnexthopserver": [ {

"name":<String_value>,

"nexthopip":<String_value>,

"nexthopfqdn":<String_value>,

"resaddresstype":<String_value>,

"nexthopport":<Integer_value>,

"secure":<String_value>,

"_nextgenapiresource":<String_value>
```

```
}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnnexthopserver/ name_value<String>
Query-parameters: attrs http:// <netscaler-ip-address> /nitro/v1/config/vpnnexthopserver/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/vpnnexthopserver/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of vpnnexthopserver resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnnexthopserver": [ {

"name":<String_value>,

"nexthopip":<String_value>,
```

```
"nexthopfqdn":<String_value>,

"resaddresstype":<String_value>,

"nexthopport":<Integer_value>,

"secure":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnnexthopserver? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vpnnexthopserver": [ { "__count": "#no"} ] }
```

vpnparameter

Configuration for VPN parameter resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
httpport	<Integer[]>	Read-write	Destination port numbers other than port 80, added as a comma-separated list. Traffic to these ports is processed as HTTP traffic, which allows functionality, such as HTTP authorization and single sign-on to a web application to work. Minimum value = 1
winsip	<String>	Read-write	WINS server IP address to add to Citrix Gateway for name resolution. Minimum length = 1
dnsvservername	<String>	Read-write	Name of the DNS virtual server for the user session. Minimum length = 1
splitdns	<String>	Read-write	Route the DNS requests to the local DNS server configured on the user device, or Citrix Gateway (remote), or both. Possible values = LOCAL, REMOTE, BOTH

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
icauseraccounting	<String>	Read-write	The name of the radiusPolicy to use for RADIUS user accounting info on the session.
sesstimeout	<Integer>	Read-write	Number of minutes after which the session times out. Default value: 30 Minimum value = 1 Maximum value = 65535
clientsecurity	<String>	Read-write	Specify the client security check for the user device to permit a Citrix Gateway session. The web address or IP address is not included in the expression for the client security check.
clientsecuritygroup	<String>	Read-write	The client security group that will be assigned on failure of the client security check. Users can in general be organized into Groups. In this case, the Client Security Group may have a more restrictive security policy. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
clientsecuritymessage	<String>	Read-write	The client security message that will be displayed on failure of the client security check. Minimum length = 1 Maximum length = 127
clientsecuritylog	<String>	Read-write	Specifies whether or not to display all failed Client Security scans to the end user. Default value: OFF Possible values = ON, OFF
smartgroup	<String>	Read-write	This is the default group that is chosen when the authentication succeeds in addition to extracted groups. Minimum length = 1 Maximum length = 64
splittunnel	<String>	Read-write	Send, through the tunnel, traffic only for intranet applications that are defined in Citrix Gateway. Route all other traffic directly to the Internet. The OFF setting routes all traffic through Citrix

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Gateway. With the REVERSE setting, intranet applications define the network traffic that is not intercepted. All network traffic directed to internal IP addresses bypasses the VPN tunnel, while other traffic goes through Citrix Gateway. Reverse split tunneling can be used to log all non-local LAN traffic. For example, if users have a home network and are logged on through the Citrix Gateway Plug-in, network traffic destined to a printer or another device within the home network is not intercepted. Default value: OFF Possible values = ON, OFF, REVERSE
locallanaccess	<String>	Read-write	Set local LAN access. If split tunneling is OFF, and you set local LAN access to ON, the local client can route traffic to its local interface. When the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			local area network switch is specified, this combination of switches is useful. The client can allow local LAN access to devices that commonly have non-routable addresses, such as local printers or local file servers. Default value: OFF Possible values = ON, OFF, FORCED
rfc1918	<String>	Read-write	As defined in the local area network, allow only the following local area network addresses to bypass the VPN tunnel when the local LAN access feature is enabled: * 10.*.*.*, * 172.16.*.*, * 192.168.*.*. Default value: OFF Possible values = ON, OFF
spoofiip	<String>	Read-write	Indicate whether or not the application requires IP spoofing, which routes the connection to the intranet application

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			through the virtual adapter. Default value: ON Possible values = ON, OFF
killconnections	<String>	Read-write	Specify whether the Citrix Gateway Plug-in should disconnect all preexisting connections, such as the connections existing before the user logged on to Citrix Gateway, and prevent new incoming connections on the Citrix Gateway Plug-in for Windows and MAC when the user is connected to Citrix Gateway and split tunneling is disabled. Default value: OFF Possible values = ON, OFF
transparentintercepti on	<String>	Read-write	Allow access to network resources by using a single IP address and subnet mask or a range of IP addresses. The OFF setting sets the mode to proxy, in which you configure destination and source IP addresses

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			and port numbers. If you are using the Citrix Gateway Plug-in for Windows, set this parameter to ON, in which the mode is set to transparent. If you are using the Citrix Gateway Plug-in for Java, set this parameter to OFF. Default value: OFF Possible values = ON, OFF
windowsclienttype	<String>	Read-write	The Windows client type. Choose between two types of Windows Client\ a) Application Agent - which always runs in the task bar as a standalone application and also has a supporting service which runs permanently when installed b) Activex Control - ActiveX control run by Microsoft Internet Explorer. Default value: AGENT

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = AGENT, PLUGIN
defaultauthorizationaction	<String>	Read-write	Specify the network resources that users have access to when they log on to the internal network. The default setting for authorization is to deny access to all network resources. Citrix recommends using the default global setting and then creating authorization policies to define the network resources users can access. If you set the default authorization policy to DENY, you must explicitly authorize access to any network resource, which improves security. Default value: DENY Possible values = ALLOW, DENY
authorizationgroup	<String>	Read-write	Comma-separated list of groups in which the user is placed when none of the groups that the user is a part of is configured on Citrix Gateway. The

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			authorization policy can be bound to these groups to control access to the resources. Minimum length = 1
clientidletimeout	<Integer>	Read-write	Time, in minutes, after which to time out the user session if Citrix Gateway does not detect mouse or keyboard activity. Minimum value = 1 Maximum value = 9999
proxy	<String>	Read-write	Set options to apply proxy for accessing the internal resources. Available settings function as follows: * BROWSER - Proxy settings are configured only in Internet Explorer and Firefox browsers. * NS - Proxy settings are configured on the Citrix ADC.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			* OFF - Proxy settings are not configured. Possible values = BROWSER, NS, OFF
allprotocolproxy	<String>	Read-write	IP address of the proxy server to use for all protocols supported by Citrix Gateway. Minimum length = 1
httpproxy	<String>	Read-write	IP address of the proxy server to be used for HTTP access for all subsequent connections to the internal network. Minimum length = 1
ftpproxy	<String>	Read-write	IP address of the proxy server to be used for FTP access for all subsequent connections to the internal network. Minimum length = 1
socksproxy	<String>	Read-write	IP address of the proxy server to be used for SOCKS access for all subsequent connections to the internal network. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
gopherproxy	<String>	Read-write	IP address of the proxy server to be used for GOPHER access for all subsequent connections to the internal network. Minimum length = 1
sslproxy	<String>	Read-write	IP address of the proxy server to be used for SSL access for all subsequent connections to the internal network. Minimum length = 1
proxyexception	<String>	Read-write	Proxy exception string that will be configured in the browser for bypassing the previously configured proxies. Allowed only if proxy type is Browser. Minimum length = 1
proxylocalbypass	<String>	Read-write	Bypass proxy server for local addresses option in Internet Explorer and Firefox proxy server settings. Default value: DISABLED Possible values = ENABLED, DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
clientcleanupprompt	<String>	Read-write	Prompt for client-side cache clean-up when a client-initiated session closes. Default value: ON Possible values = ON, OFF
forcecleanup	<String[]>	Read-write	Force cache clean-up when the user closes a session. You can specify all, none, or any combination of the client-side items. Possible values = none, all, cookie, addressbar, plugin, filesystemapplicatio n, application, applicationdata, clientcertificate, autocomplete, cache
clientoptions	<String[]>	Read-write	Display only the configured menu options when you select the "Configure Citrix Gateway" option in the Citrix Gateway Plug-in's system tray icon for Windows. Possible values = none, all, services,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			filetransfer, configuration
clientconfiguration	<String[]>	Read-write	Allow users to change client Debug logging level in Configuration tab of the Citrix Gateway Plug-in for Windows. Possible values = none, trace
sso	<String>	Read-write	Set single sign-on (SSO) for the session. When the user accesses a server, the user's logon credentials are passed to the server for authentication. NOTE : This configuration does not honor the following authentication types for security reason. BASIC, DIGEST, and NTLM (without Negotiate NTLM2 Key or Negotiate Sign Flag). Use VPN TrafficAction to configure SSO for these authentication types. Default value: OFF

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ON, OFF
ssocredential	<String>	Read-write	Specify whether to use the primary or secondary authentication credentials for single sign-on to the server. Default value: PRIMARY Possible values = PRIMARY, SECONDARY
windowsautologon	<String>	Read-write	Enable or disable the Windows Auto Logon for the session. If a VPN session is established after this setting is enabled, the user is automatically logged on by using Windows credentials after the system is restarted. Default value: OFF Possible values = ON, OFF
usemip	<String>	Read-write	Enable or disable the use of a unique IP address alias, or a mapped IP address, as the client IP address for each client session. Allow Citrix Gateway to use the mapped IP

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			address as an intranet IP address when all other IP addresses are not available. When IP pooling is configured and the mapped IP is used as an intranet IP address, the mapped IP address is used when an intranet IP address cannot be assigned. Default value: NS Possible values = NS, OFF
useiip	<String>	Read-write	Define IP address pool options. Available settings function as follows: * SPILLOVER - When an address pool is configured and the mapped IP is used as an intranet IP address, the mapped IP address is used when an intranet IP address cannot be assigned.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			* NOSPILLOVER - When intranet IP addresses are enabled and the mapped IP address is not used, the Transfer Login page appears for users who have used all available intranet IP addresses. * OFF - Address pool is not configured. Default value: NOSPILLOVER Possible values = NOSPILLOVER, SPILLOVER, OFF
clientdebug	<String>	Read-write	Set the trace level on Citrix Gateway. Technical support technicians use these debug logs for in-depth debugging and troubleshooting purposes. Available settings function as follows: * DEBUG - Detailed debug messages are collected and written into the specified file.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			* STATS - Application audit level error messages and debug statistic counters are written into the specified file. * EVENTS - Application audit-level error messages are written into the specified file. * OFF - Only critical events are logged into the Windows Application Log. Default value: OFF Possible values = debug, stats, events, OFF
loginscript	<String>	Read-write	Path to the logon script that is run when a session is established. Separate multiple scripts by using comma. A "$" in the path signifies that the word following the "$" is an environment variable. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
logoutscript	<String>	Read-write	Path to the logout script. Separate multiple scripts by using comma. A "$" in the path signifies that the word following the "$" is an environment variable. Minimum length = 1
homepage	<String>	Read-write	Web address of the home page that appears when users log on. Otherwise, users receive the default home page for Citrix Gateway, which is the Access Interface.
icaproxy	<String>	Read-write	Enable ICA proxy to configure secure Internet access to servers running Citrix XenApp or XenDesktop by using Citrix Receiver instead of the Citrix Gateway Plug-in. Default value: OFF Possible values = ON, OFF
wihome	<String>	Read-write	Web address of the Web Interface server, such as http://<ipAddress>/Citrix/XenApp, or Receiver for Web,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			which enumerates the virtualized resources, such as XenApp, XenDesktop, and cloud applications. This web address is used as the home page in ICA proxy mode. If Client Choices is ON, you must configure this setting. Because the user can choose between FullClient and ICAProxy, the user may see a different home page. An Internet web site may appear if the user gets the FullClient option, or a Web Interface site if the user gets the ICAProxy option. If the setting is not configured, the XenApp option does not appear as a client choice.
wihomeaddresstype	<String>	Read-write	Type of the wihome address(IPV4/V6). Possible values = IPV4, IPV6

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
citrixreceiverhome	<String>	Read-write	Web address for the Citrix Receiver home page. Configure Citrix Gateway so that when users log on to the appliance, the Citrix Gateway Plug-in opens a web browser that allows single sign-on to the Citrix Receiver home page.
wiportalmode	<String>	Read-write	Layout on the Access Interface. The COMPACT value indicates the use of small icons. Possible values = NORMAL, COMPACT
clientchoices	<String>	Read-write	Provide users with multiple logon options. With client choices, users have the option of logging on by using the Citrix Gateway Plug-in for Windows, Citrix Gateway Plug-in for Java, the Web Interface, or clientless access from one location. Depending on how Citrix Gateway is configured, users are presented with up to three icons for logon

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			choices. The most common are the Citrix Gateway Plug-in for Windows, Web Interface, and clientless access. Default value: OFF Possible values = ON, OFF
epaclienttype	<String>	Read-write	Choose between two types of End point Windows Client a) Application Agent - which always runs in the task bar as a standalone application and also has a supporting service which runs permanently when installed b) Activex Control - ActiveX control run by Microsoft Internet Explorer. Possible values = AGENT, PLUGIN
iipdnssuffix	<String>	Read-write	An intranet IP DNS suffix. When a user logs on to Citrix Gateway and is assigned an IP address, a DNS record for the user name and IP

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			address combination is added to the Citrix Gateway DNS cache. You can configure a DNS suffix to append to the user name when the DNS record is added to the cache. You can reach to the host from where the user is logged on by using the user's name, which can be easier to remember than an IP address. When the user logs off from Citrix Gateway, the record is removed from the DNS cache. Minimum length = 1
forcedtimeout	<Integer>	Read-write	Force a disconnection from the Citrix Gateway Plug-in with Citrix Gateway after a specified number of minutes. If the session closes, the user must log on again. Minimum value = 1 Maximum value = 65535
forcedtimeoutwarning	<Integer>	Read-write	Number of minutes to warn a user before

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			the user session is disconnected. Minimum value = 1 Maximum value = 255
ntdomain	<String>	Read-write	Single sign-on domain to use for single sign-on to applications in the internal network. This setting can be overwritten by the domain that users specify at the time of logon or by the domain that the authentication server returns. Minimum length = 1 Maximum length = 32
clientlessvpnmode	<String>	Read-write	Enable clientless access for web, XenApp or XenDesktop, and FileShare resources without installing the Citrix Gateway Plug-in. Available settings function as follows: * ON - Allow only clientless access. * OFF - Allow clientless access after users log on

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			with the Citrix Gateway Plug-in. * DISABLED - Do not allow clientless access. Default value: OFF Possible values = ON, OFF, DISABLED
clientlessmodeurlencoding	<String>	Read-write	When clientless access is enabled, you can choose to encode the addresses of internal web applications or to leave the address as clear text. Available settings function as follows: * OPAQUE - Use standard encoding mechanisms to make the domain and protocol part of the resource unclear to users. * TRANSPARENT - Do not encode the web address and make it visible to users.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			* ENCRYPT - Allow the domain and protocol to be encrypted using a session key. When the web address is encrypted, the URL is different for each user session for the same web resource. If users bookmark the encoded web address, save it in the web browser and then log off, they cannot connect to the web address when they log on and use the bookmark. If users save the encrypted bookmark in the Access Interface during their session, the bookmark works each time the user logs on. Default value: OPAQUE Possible values = TRANSPARENT, OPAQUE, ENCRYPT

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
clientlesspersistentcookie	<String>	Read-write	State of persistent cookies in clientless access mode. Persistent cookies are required for accessing certain features of SharePoint, such as opening and editing Microsoft Word, Excel, and PowerPoint documents hosted on the SharePoint server. A persistent cookie remains on the user device and is sent with each HTTP request. Citrix Gateway encrypts the persistent cookie before sending it to the plug-in on the user device, and refreshes the cookie periodically as long as the session exists. The cookie becomes stale if the session ends. Available settings function as follows: * ALLOW - Enable persistent cookies. Users can open and edit Microsoft documents stored in SharePoint.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			* DENY - Disable persistent cookies. Users cannot open and edit Microsoft documents stored in SharePoint. * PROMPT - Prompt users to allow or deny persistent cookies during the session. Persistent cookies are not required for clientless access if users do not connect to SharePoint. Default value: DENY Possible values = ALLOW, DENY, PROMPT
emailhome	<String>	Read-write	Web address for the web-based email, such as Outlook Web Access.
allowedlogingroups	<String>	Read-write	Specify groups that have permission to log on to Citrix Gateway. Users who do not belong to this group or groups are denied access even

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			if they have valid credentials. Minimum length = 1 Maximum length = 511
encryptcsecexp	<String>	Read-write	Enable encryption of client security expressions. Default value: ENABLED Possible values = ENABLED, DISABLED
apptokentimeout	<Integer>	Read-write	The timeout value in seconds for tokens to access XenMobile applications. Default value: 100 Minimum value = 1 Maximum value = 255
mdxtokentimeout	<Integer>	Read-write	Validity of MDX Token in minutes. This token is used for mdx services to access backend and valid HEAD and GET request. Default value: 10 Minimum value = 1 Maximum value = 1440

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
uitheme	<String>	Read-write	Set VPN UI Theme to Green-Bubble, Caxton or Custom; default is Caxton. Possible values = DEFAULT, GREENBUBBLE, CUSTOM
securebrowse	<String>	Read-write	Allow users to connect through Citrix Gateway to network resources from iOS and Android mobile devices with Citrix Receiver. Users do not need to establish a full VPN tunnel to access resources in the secure network. Default value: ENABLED Possible values = ENABLED, DISABLED
storefronturl	<String>	Read-write	Web address for StoreFront to be used in this session for enumeration of resources from XenApp or XenDesktop. Minimum length = 1 Maximum length = 255

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
kcdaccount	<String>	Read-write	The KCD account details to be used in SSO.
clientversions	<String>	Read-write	checkversion api. Minimum length = 1 Maximum length = 100
rdpclientprofilename	<String>	Read-write	Name of the RDP profile associated with the vserver. Minimum length = 1 Maximum length = 127
windowspluginupgrade	<String>	Read-write	Option to set plugin upgrade behaviour for Win. Default value: Always Possible values = Always, Essential, Never
macpluginupgrade	<String>	Read-write	Option to set plugin upgrade behaviour for Mac. Default value: Always Possible values = Always, Essential, Never

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
linuxpluginupgrade	<String>	Read-write	Option to set plugin upgrade behaviour for Linux. Default value: Always Possible values = Always, Essential, Never
iconwithreceiver	<String>	Read-write	Option to decide whether to show plugin icon along with receiver icon. Default value: OFF Possible values = ON, OFF
userdomains	<String>	Read-write	List of user domains specified as comma seperated value.
icasessiontimeout	<String>	Read-write	Enable or disable ica session timeout. If enabled and in case AAA session gets terminated, ICA connections associated with that will also get terminated. Default value: OFF Possible values = ON, OFF
httptrackconnproxy	<String>	Read-write	Use separate TCP connections for each connection proxy

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			request in GSLB Active-Active setups. Improves session isolation but may impact performance due to increased connections and TLS overhead. Disabled by default. Default value: OFF Possible values = ON, OFF
alwaysonprofilename	<String>	Read-write	Name of the AlwaysON profile. The builtin profile named none can be used to explicitly disable AlwaysON. Minimum length = 1 Maximum length = 127
autoproxyurl	<String>	Read-write	URL to auto proxy config file.
advancedclientlessvpnmode	<String>	Read-write	Option to enable/disable Advanced ClientlessVpnMode. Additionaly, it can be set to STRICT to block Classic ClientlessVpnMode while in AdvancedClientless Mode. Default value: DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ENABLED, DISABLED, STRICT
pcoipprofilename	<String>	Read-write	Name of the PCOIP profile. Minimum length = 1 Maximum length = 127
backendserversni	<String>	Read-write	enables sni extension for backend server handshakes. Default value: DISABLED Possible values = ENABLED, DISABLED
backendcertvalidation	<String>	Read-write	enables backend server certificate validation. Default value: DISABLED Possible values = ENABLED, DISABLED
secureprivateaccess	<String>	Read-write	Enables or disables the secure private access configuration. Default value: DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ENABLED, DISABLED
accessrestrictedpage redirect	<String>	Read-write	By default, an access restricted page hosted on secure private access CDN is displayed when a restricted app is accessed. The setting can be changed to NS to display the access restricted page hosted on the gateway or OFF to not display any access restricted page. Default value: CDN Possible values = CDN, NS, OFF
fqdnspoofedip	<String>	Read-write	Spoofed IP address range that can be used by client for FQDN based split tunneling. Minimum length = 1
netmask	<String>	Read-write	The netmask for the spoofed ip address. Minimum length = 1
samesite	<String>	Read-write	SameSite attribute value for Cookies generated in VPN context. This

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			attribute value will be appended only for the cookies which are specified in the builtin patset ns_cookies_samesite. Possible values = None, LAX, STRICT
maxiipperuser	<Integer>	Read-write	Maximum number of Intranet IP that can be assigned to a user from AAA group, VPN vserver or VPN global pool. This setting is not applicable for AAA user level Intranet IP configuration. Default value: 1 Minimum value = 1 Maximum value = 10
deviceposture	<String>	Read-write	Enable device posture. Default value: DISABLED Possible values = ENABLED, DISABLED
backenddtls12	<String>	Read-write	Enables DTLS 1.2 for backend server handshakes.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: DISABLED Possible values = ENABLED, DISABLED
secureprivateaccessprofile	<String>	Read-write	Clears Secure Private Access profile that may be set.
name	<String>	Read-only	The VPN name.
clientidletimeoutwarning	<Integer>	Read-only	The time after which the client gets a timeout warning, in minutes.
stricturlcheck	<String>	Read-only	Enables or disables the strict endpoint or URL checking with respect to the configuration. Default value: ENABLED Possible values = ENABLED, DISABLED
vpnsessionpolicybindtype	<String>	Read-only	Indicates current bind type (Classic/ Advanced) for VPN session policy across all bind entities. Default value: Advanced Policy

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = Classic Policy, Advanced Policy
vpnsessionpolicycount	<Integer>	Read-only	Count of VPN session policies across all bind entities.
_nextgenapiresource	<String>	Read-only	.

Operations

(click to see Properties)

- UPDATE
- UNSET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnparameter **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"vpnparameter":{

"httpport":<Integer[]_value>,

"winsip":<String_value>,

"dnsvservername":<String_value>,

"splitdns":<String_value>,

"icauseraccounting":<String_value>,

"sesstimeout":<Integer_value>,

"clientsecurity":<String_value>,

"clientsecuritygroup":<String_value>,

"clientsecuritymessage":<String_value>,

"clientsecuritylog":<String_value>,

"smartgroup":<String_value>,

"splittunnel":<String_value>,

"locallanaccess":<String_value>,
```

```
"rfc1918":<String_value>,

"spoofiip":<String_value>,

"killconnections":<String_value>,

"transparentinterception":<String_value>,

"windowsclienttype":<String_value>,

"defaultauthorizationaction":<String_value>,

"authorizationgroup":<String_value>,

"clientidletimeout":<Integer_value>,

"proxy":<String_value>,

"allprotocolproxy":<String_value>,

"httpproxy":<String_value>,

"ftpproxy":<String_value>,

"socksproxy":<String_value>,

"gopherproxy":<String_value>,

"sslproxy":<String_value>,

"proxyexception":<String_value>,

"proxylocalbypass":<String_value>,

"clientcleanupprompt":<String_value>,

"forcecleanup":<String[]_value>,

"clientoptions":<String[]_value>,

"clientconfiguration":<String[]_value>,

"sso":<String_value>,
```

```
"ssocredential":<String_value>,

"windowsautologon":<String_value>,

"usemip":<String_value>,

"useiip":<String_value>,

"clientdebug":<String_value>,

"loginscript":<String_value>,

"logoutscript":<String_value>,

"homepage":<String_value>,

"icaproxy":<String_value>,

"wihome":<String_value>,

"wihomeaddresstype":<String_value>,

"citrixreceiverhome":<String_value>,

"wiportalmode":<String_value>,

"clientchoices":<String_value>,

"epaclienttype":<String_value>,

"iipdnssuffix":<String_value>,

"forcedtimeout":<Integer_value>,

"forcedtimeoutwarning":<Integer_value>,

"ntdomain":<String_value>,

"clientlessvpnmode":<String_value>,

"clientlessmodeurlencoding":<String_value>,

"clientlesspersistentcookie":<String_value>,
```

```
"emailhome":<String_value>,

"allowedlogingroups":<String_value>,

"encryptcsecexp":<String_value>,

"apptokentimeout":<Integer_value>,

"mdxtokentimeout":<Integer_value>,

"uitheme":<String_value>,

"securebrowse":<String_value>,

"storefronturl":<String_value>,

"kcdaccount":<String_value>,

"clientversions":<String_value>,

"rdpclientprofilename":<String_value>,

"windowspluginupgrade":<String_value>,

"macpluginupgrade":<String_value>,

"linuxpluginupgrade":<String_value>,

"iconwithreceiver":<String_value>,

"userdomains":<String_value>,

"icasessiontimeout":<String_value>,

"httptrackconnproxy":<String_value>,

"alwaysonprofilename":<String_value>,

"autoproxyurl":<String_value>,

"advancedclientlessvpnmode":<String_value>,

"pcoipprofilename":<String_value>,
```

```
"backendserversni":<String_value>,

"backendcertvalidation":<String_value>,

"secureprivateaccess":<String_value>,

"accessrestrictedpageredirect":<String_value>,

"fqdnspoofedip":<String_value>,

"netmask":<String_value>,

"samesite":<String_value>,

"maxiipperuser":<Integer_value>,

"deviceposture":<String_value>,

"backenddtls12":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnparameter? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"vpnparameter":{

"httpport":true,

"winsip":true,

"dnsvservername":true,

"splitdns":true,

"icauseraccounting":true,

"sesstimeout":true,

"clientsecurity":true,

"clientsecuritygroup":true,

"smartgroup":true,

"clientsecuritymessage":true,

"clientsecuritylog":true,

"authorizationgroup":true,

"clientidletimeout":true,

"allprotocolproxy":true,

"httpproxy":true,

"ftpproxy":true,

"socksproxy":true,

"gopherproxy":true,

"sslproxy":true,

"proxyexception":true,

"forcecleanup":true,
```

```
"clientoptions":true,

"clientconfiguration":true,

"loginscript":true,

"logoutscript":true,

"homepage":true,

"proxy":true,

"wihome":true,

"citrixreceiverhome":true,

"wiportalmode":true,

"iipdnssuffix":true,

"forcedtimeout":true,

"forcedtimeoutwarning":true,

"defaultauthorizationaction":true,

"ntdomain":true,

"clientlessvpnmode":true,

"emailhome":true,

"clientlessmodeurlencoding":true,

"clientlesspersistentcookie":true,

"allowedlogingroups":true,

"apptokentimeout":true,

"mdxtokentimeout":true,

"storefronturl":true,
```

```
"uitheme":true,

"kcdaccount":true,

"rdpclientprofilename":true,

"windowspluginupgrade":true,

"macpluginupgrade":true,

"linuxpluginupgrade":true,

"iconwithreceiver":true,

"userdomains":true,

"alwaysonprofilename":true,

"autoproxyurl":true,

"pcoipprofilename":true,

"advancedclientlessvpnmode":true,

"fqdnspoofedip":true,

"secureprivateaccess":true,

"accessrestrictedpageredirect":true,

"secureprivateaccessprofile":true,

"splittunnel":true,

"locallanaccess":true,

"rfc1918":true,

"spoofiip":true,

"killconnections":true,

"transparentinterception":true,
```

```
"windowsclienttype":true,

"proxylocalbypass":true,

"clientcleanupprompt":true,

"sso":true,

"ssocredential":true,

"windowsautologon":true,

"usemip":true,

"useiip":true,

"clientdebug":true,

"icaproxy":true,

"clientchoices":true,

"epaclienttype":true,

"encryptcsecexp":true,

"securebrowse":true,

"clientversions":true,

"icasessiontimeout":true,

"httptrackconnproxy":true,

"backendserversni":true,

"backendcertvalidation":true,

"netmask":true,

"samesite":true,

"maxiipperuser":true,
```

```
"deviceposture":true,

"backenddtls12":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnparameter **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vpnparameter": [ {

"name":<String_value>,

"httpport":<Integer[]_value>,

"winsip":<String_value>,

"dnsvservername":<String_value>,

"splitdns":<String_value>,
```

```
"icauseraccounting":<String_value>,

"sesstimeout":<Integer_value>,

"clientsecurity":<String_value>,

"clientsecuritygroup":<String_value>,

"clientsecuritymessage":<String_value>,

"clientsecuritylog":<String_value>,

"smartgroup":<String_value>,

"splittunnel":<String_value>,

"locallanaccess":<String_value>,

"rfc1918":<String_value>,

"spoofiip":<String_value>,

"killconnections":<String_value>,

"transparentinterception":<String_value>,

"windowsclienttype":<String_value>,

"defaultauthorizationaction":<String_value>,

"authorizationgroup":<String_value>,

"clientidletimeout":<Integer_value>,

"clientidletimeoutwarning":<Integer_value>,

"proxy":<String_value>,

"allprotocolproxy":<String_value>,

"httpproxy":<String_value>,

"ftpproxy":<String_value>,
```

```
"socksproxy":<String_value>,

"gopherproxy":<String_value>,

"sslproxy":<String_value>,

"proxyexception":<String_value>,

"proxylocalbypass":<String_value>,

"clientcleanupprompt":<String_value>,

"forcecleanup":<String[]_value>,

"clientoptions":<String[]_value>,

"clientconfiguration":<String[]_value>,

"sso":<String_value>,

"ssocredential":<String_value>,

"windowsautologon":<String_value>,

"usemip":<String_value>,

"useiip":<String_value>,

"clientdebug":<String_value>,

"loginscript":<String_value>,

"logoutscript":<String_value>,

"homepage":<String_value>,

"icaproxy":<String_value>,

"wihome":<String_value>,

"wihomeaddresstype":<String_value>,

"citrixreceiverhome":<String_value>,
```

```
"wiportalmode":<String_value>,

"clientchoices":<String_value>,

"epaclienttype":<String_value>,

"iipdnssuffix":<String_value>,

"forcedtimeout":<Integer_value>,

"forcedtimeoutwarning":<Integer_value>,

"ntdomain":<String_value>,

"clientlessvpnmode":<String_value>,

"clientlessmodeurlencoding":<String_value>,

"clientlesspersistentcookie":<String_value>,

"emailhome":<String_value>,

"allowedlogingroups":<String_value>,

"encryptcsecexp":<String_value>,

"apptokentimeout":<Integer_value>,

"mdxtokentimeout":<Integer_value>,

"uitheme":<String_value>,

"securebrowse":<String_value>,

"storefronturl":<String_value>,

"kcdaccount":<String_value>,

"clientversions":<String_value>,

"rdpclientprofilename":<String_value>,

"windowspluginupgrade":<String_value>,
```

```
"macpluginupgrade":<String_value>,

"linuxpluginupgrade":<String_value>,

"iconwithreceiver":<String_value>,

"userdomains":<String_value>,

"icasessiontimeout":<String_value>,

"httptrackconnproxy":<String_value>,

"alwaysonprofilename":<String_value>,

"autoproxyurl":<String_value>,

"advancedclientlessvpnmode":<String_value>,

"pcoipprofilename":<String_value>,

"backendserversni":<String_value>,

"backendcertvalidation":<String_value>,

"secureprivateaccess":<String_value>,

"stricturlcheck":<String_value>,

"accessrestrictedpageredirect":<String_value>,

"vpnsessionpolicybindtype":<String_value>,

"vpnsessionpolicycount":<Integer_value>,

"fqdnspoofedip":<String_value>,

"netmask":<String_value>,

"samesite":<String_value>,

"maxiipperuser":<Integer_value>,

"deviceposture":<String_value>,
```

```
"backenddtls12":<String_value>,

"secureprivateaccessprofile":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

vpnpcoipconnection

Configuration for PCoIP connection resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
username	<String>	Read-write	User name for the PCOIP connections. Minimum length = 1
nodeid	<Integer>	Read-write	Unique number that identifies the cluster node. Minimum value = 0 Maximum value = 31
all	<Boolean>	Read-write	All active pcoip connections.
srcip	<String>	Read-only	The client IP address.
srcport	<Integer>	Read-only	The client port. Range 1 - 65535 * in CLI is represented as

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			65535 in NITRO API
destip	<String>	Read-only	The VDA IP address.
destport	<Integer>	Read-only	The VDA server port. Range 1 - 65535 * in CLI is represented as 65535 in NITRO API
peid	<Integer>	Read-only	Core id of the session owner.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET (ALL)
- COUNT
- KILL

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of

creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

KILL

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnpcoipconnection? **action=kill HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"vpnpcoipconnection":{

"username":<String_value>,

"all":<Boolean_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnpcoipconnection **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/vpnpcoipconnection? **args=username: <String_value> ,nodeid: <Integer_value>**

Use this query-parameter to get vpnpcoipconnection resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/config/vpnpcoipconnection? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/vpnpcoipconnection? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of vpnpcoipconnection resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/vpnpcoipconnection? **view=summary**

Use this query-parameter to get the summary output of vpnpcoipconnection resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/vpnpcoipconnection? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vpnpcoipconnection resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vpnpcoipconnection": [ {

username:<String_value>,nodeid:<Integer_value>"srcip":<String_value>,

"srcport":<Integer_value>,

"destip":<String_value>,

"destport":<Integer_value>,

"peid":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnpcoipconnection? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vpnpcoipconnection": [ { "__count": "#no"} ] }
```

vpnpcoipprofile

Configuration for PCoIP session profile resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	name of PCoIP profile. Minimum length = 1
conserverurl	<String>	Read-write	Connection server URL.
icvverification	<String>	Read-write	ICV verification for PCOIP transport packets. Default value: DISABLED Possible values = ENABLED, DISABLED
sessionidletimeout	<Integer>	Read-write	PCOIP Idle Session timeout. Default value: 180 Minimum value = 30 Maximum value = 240
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnpcoipprofile **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"vpnpcoipprofile":{

<b>"name":<String_value>,

</b><b>"conserverurl":<String_value>,

</b>"icvverification":<String_value>,

"sessionidletimeout":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnpcoipprofile/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnpcoipprofile **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"vpnpcoipprofile":{

<b>"name":<String_value>,

</b>"conserverurl":<String_value>,

"icvverification":<String_value>,

"sessionidletimeout":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnpcoipprofile? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"vpnpcoipprofile":{

<b>"name":<String_value>,

</b>"icvverification":true,

"sessionidletimeout":true
```

```
}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnpcoipprofile **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/vpnpcoipprofile? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/vpnpcoipprofile? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of vpnpcoipprofile resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/vpnpcoipprofile? **view=summary**

Use this query-parameter to get the summary output of vpnpcoipprofile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/vpnpcoipprofile? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vpnpcoipprofile resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vpnpcoipprofile": [ {

"name":<String_value>,

"conserverurl":<String_value>,

"icvverification":<String_value>,

"sessionidletimeout":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnpcoipprofile/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/vpnpcoipprofile/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/vpnpcoipprofile/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of vpnpcoipprofile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnpcoipprofile": [ {

"name":<String_value>,

"conserverurl":<String_value>,

"icvverification":<String_value>,

"sessionidletimeout":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnpcoipprofile? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vpnpcoipprofile": [ { "__count": "#no"} ] }
```

vpnpcoipvserverprofile

Configuration for PCoIP vserver profile resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	name of PCoIP vserver profile. Minimum length = 1
logindomain	<String>	Read-write	Login domain for PCoIP users.
udpport	<Integer>	Read-write	UDP port for PCoIP data traffic. Default value: 4172 Range 1 - 65535 * in CLI is represented as 65535 in NITRO API
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnpcoipvserverprofile **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"vpnpcoipvserverprofile":{

<b>"name":<String_value>,

</b><b>"logindomain":<String_value>,

</b>"udpport":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnpcoipvserverprofile/ name_value<String>
HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnpcoipvserverprofile **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"vpnpcoipvserverprofile":{

<b>"name":<String_value>,

</b>"udpport":<Integer_value>,

"logindomain":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnpcoipvserverprofile? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"vpnpcoipvserverprofile":{

<b>"name":<String_value>,

</b>"udpport":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnpcoipvserverprofile **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/vpnpcoipvserverprofile? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/vpnpcoipvserverprofile? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of vpnpcoipvserverprofile resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/vpnpcoipvserverprofile? **view=summary**

Use this query-parameter to get the summary output of vpnpcoipvserverprofile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/vpnpcoipvserverprofile? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vpnpcoipvserverprofile resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vpnpcoipvserverprofile": [ {

"name":<String_value>,

"udpport":<Integer_value>,

"logindomain":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnpcoipvserverprofile/ name_value<String>
Query-parameters: attrs http:// <netscaler-ip-address> /nitro/v1/config/vpnpcoipvserverprofile/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/vpnpcoipvserverprofile/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of vpnpcoipvserverprofile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnpcoipvserverprofile": [ {

"name":<String_value>,

"udpport":<Integer_value>,

"logindomain":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnpcoipvserverprofile? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vpnpcoipvserverprofile": [ { "__count": "#no"} ] }
```

vpnportaltheme

Configuration for portaltheme resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the uitheme. Minimum length = 1
basetheme	<String>	Read-write	. Minimum length = 1 Possible values = Default, Greenbubble, X1, RfWebUI, WStheme
feature	<String>	Read-only	The feature to be checked while applying this config.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnportaltheme **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"vpnportaltheme":{

<b>"name":<String_value>,

</b><b>"basetheme":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnportaltheme/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnportaltheme **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/vpnportaltheme? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/vpnportaltheme? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of vpnportaltheme resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/vpnportaltheme? **view=summary**

Use this query-parameter to get the summary output of vpnportaltheme resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/vpnportaltheme? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vpnportaltheme resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vpnportaltheme": [ {

"name":<String_value>,

"basetheme":<String_value>,

"feature":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnportaltheme/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/vpnportaltheme/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/vpnportaltheme/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of vpnportaltheme resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnportaltheme": [ {

"name":<String_value>,

"basetheme":<String_value>,

"feature":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnportaltheme? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vpnportaltheme": [ { "__count": "#no"} ] }
```

vpnsamlssoprofile

Configuration for SAML sso action resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the new saml single sign-on profile. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after an SSO action is created.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my action" or 'my action'). Minimum length = 1
samlsigningcertname	<String>	Read-write	Name of the signing authority as given in the SAML server's SSL certificate. Minimum length = 1
assertionconsumerserviceurl	<String>	Read-write	URL to which the assertion is to be sent. Minimum length = 1
relaystaterule	<String>	Read-write	Expression to extract relaystate to be sent along with assertion. Evaluation of this expression should return TEXT content. This is typically a target url to which user is redirected after the recipient validates SAML token.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
sendpassword	<String>	Read-write	Option to send password in assertion. Default value: OFF Possible values = ON, OFF
samlissuername	<String>	Read-write	The name to be used in requests sent from Citrix ADC to IdP to uniquely identify Citrix ADC. Minimum length = 1
signaturealg	<String>	Read-write	Algorithm to be used to sign/verify SAML transactions. Default value: RSA-SHA256 Possible values = RSA-SHA1, RSA-SHA256
digestmethod	<String>	Read-write	Algorithm to be used to compute/verify digest for SAML transactions. Default value: SHA256 Possible values = SHA1, SHA256
audience	<String>	Read-write	Audience for which assertion sent by IdP is applicable. This is typically entity name

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			or url that represents ServiceProvider.
nameidformat	<String>	Read-write	Format of Name Identifier sent in Assertion. Default value: transient Possible values = Unspecified, emailAddress, X509SubjectName, WindowsDomainQualifiedName, kerberos, entity, persistent, transient
nameidexpr	<String>	Read-write	Expression that will be evaluated to obtain NameIdentifier to be sent in assertion. Maximum length = 128
attribute1	<String>	Read-write	Name of attribute1 that needs to be sent in SAML Assertion.
attribute1expr	<String>	Read-write	Expression that will be evaluated to obtain attribute1's value to be sent in Assertion. Maximum length = 128

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
attribute1friendlyname	<String>	Read-write	User-Friendly Name of attribute1 that needs to be sent in SAML Assertion.
attribute1format	<String>	Read-write	Format of Attribute1 to be sent in Assertion. Possible values = URI, Basic
attribute2	<String>	Read-write	Name of attribute2 that needs to be sent in SAML Assertion.
attribute2expr	<String>	Read-write	Expression that will be evaluated to obtain attribute2's value to be sent in Assertion. Maximum length = 128
attribute2friendlyname	<String>	Read-write	User-Friendly Name of attribute2 that needs to be sent in SAML Assertion.
attribute2format	<String>	Read-write	Format of Attribute2 to be sent in Assertion. Possible values = URI, Basic
attribute3	<String>	Read-write	Name of attribute3 that needs to be sent in SAML Assertion.
attribute3expr	<String>	Read-write	Expression that will be evaluated to

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			obtain attribute3's value to be sent in Assertion. Maximum length = 128
attribute3friendlyname	<String>	Read-write	User-Friendly Name of attribute3 that needs to be sent in SAML Assertion.
attribute3format	<String>	Read-write	Format of Attribute3 to be sent in Assertion. Possible values = URI, Basic
attribute4	<String>	Read-write	Name of attribute4 that needs to be sent in SAML Assertion.
attribute4expr	<String>	Read-write	Expression that will be evaluated to obtain attribute4's value to be sent in Assertion. Maximum length = 128
attribute4friendlyname	<String>	Read-write	User-Friendly Name of attribute4 that needs to be sent in SAML Assertion.
attribute4format	<String>	Read-write	Format of Attribute4 to be sent in Assertion. Possible values = URI, Basic

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
attribute5	<String>	Read-write	Name of attribute5 that needs to be sent in SAML Assertion.
attribute5expr	<String>	Read-write	Expression that will be evaluated to obtain attribute5's value to be sent in Assertion. Maximum length = 128
attribute5friendlyname	<String>	Read-write	User-Friendly Name of attribute5 that needs to be sent in SAML Assertion.
attribute5format	<String>	Read-write	Format of Attribute5 to be sent in Assertion. Possible values = URI, Basic
attribute6	<String>	Read-write	Name of attribute6 that needs to be sent in SAML Assertion.
attribute6expr	<String>	Read-write	Expression that will be evaluated to obtain attribute6's value to be sent in Assertion. Maximum length = 128
attribute6friendlyname	<String>	Read-write	User-Friendly Name of attribute6 that needs to be sent in SAML Assertion.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
attribute6format	<String>	Read-write	Format of Attribute6 to be sent in Assertion. Possible values = URI, Basic
attribute7	<String>	Read-write	Name of attribute7 that needs to be sent in SAML Assertion.
attribute7expr	<String>	Read-write	Expression that will be evaluated to obtain attribute7's value to be sent in Assertion. Maximum length = 128
attribute7friendlyname	<String>	Read-write	User-Friendly Name of attribute7 that needs to be sent in SAML Assertion.
attribute7format	<String>	Read-write	Format of Attribute7 to be sent in Assertion. Possible values = URI, Basic
attribute8	<String>	Read-write	Name of attribute8 that needs to be sent in SAML Assertion.
attribute8expr	<String>	Read-write	Expression that will be evaluated to obtain attribute8's value to be sent in Assertion. Maximum length = 128

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
attribute8friendlyname	<String>	Read-write	User-Friendly Name of attribute8 that needs to be sent in SAML Assertion.
attribute8format	<String>	Read-write	Format of Attribute8 to be sent in Assertion. Possible values = URI, Basic
attribute9	<String>	Read-write	Name of attribute9 that needs to be sent in SAML Assertion.
attribute9expr	<String>	Read-write	Expression that will be evaluated to obtain attribute9's value to be sent in Assertion. Maximum length = 128
attribute9friendlyname	<String>	Read-write	User-Friendly Name of attribute9 that needs to be sent in SAML Assertion.
attribute9format	<String>	Read-write	Format of Attribute9 to be sent in Assertion. Possible values = URI, Basic
attribute10	<String>	Read-write	Name of attribute10 that needs to be sent in SAML Assertion.
attribute10expr	<String>	Read-write	Expression that will be evaluated to

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			obtain attribute10's value to be sent in Assertion. Maximum length = 128
attribute10friendlyname	<String>	Read-write	User-Friendly Name of attribute10 that needs to be sent in SAML Assertion.
attribute10format	<String>	Read-write	Format of Attribute10 to be sent in Assertion. Possible values = URI, Basic
attribute11	<String>	Read-write	Name of attribute11 that needs to be sent in SAML Assertion.
attribute11expr	<String>	Read-write	Expression that will be evaluated to obtain attribute11's value to be sent in Assertion. Maximum length = 128
attribute11friendlyname	<String>	Read-write	User-Friendly Name of attribute11 that needs to be sent in SAML Assertion.
attribute11format	<String>	Read-write	Format of Attribute11 to be sent in Assertion. Possible values = URI, Basic

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
attribute12	<String>	Read-write	Name of attribute12 that needs to be sent in SAML Assertion.
attribute12expr	<String>	Read-write	Expression that will be evaluated to obtain attribute12's value to be sent in Assertion. Maximum length = 128
attribute12friendlyname	<String>	Read-write	User-Friendly Name of attribute12 that needs to be sent in SAML Assertion.
attribute12format	<String>	Read-write	Format of Attribute12 to be sent in Assertion. Possible values = URI, Basic
attribute13	<String>	Read-write	Name of attribute13 that needs to be sent in SAML Assertion.
attribute13expr	<String>	Read-write	Expression that will be evaluated to obtain attribute13's value to be sent in Assertion. Maximum length = 128
attribute13friendlyname	<String>	Read-write	User-Friendly Name of attribute13 that needs to be sent in SAML Assertion.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
attribute13format	<String>	Read-write	Format of Attribute13 to be sent in Assertion. Possible values = URI, Basic
attribute14	<String>	Read-write	Name of attribute14 that needs to be sent in SAML Assertion.
attribute14expr	<String>	Read-write	Expression that will be evaluated to obtain attribute14's value to be sent in Assertion. Maximum length = 128
attribute14friendlyname	<String>	Read-write	User-Friendly Name of attribute14 that needs to be sent in SAML Assertion.
attribute14format	<String>	Read-write	Format of Attribute14 to be sent in Assertion. Possible values = URI, Basic
attribute15	<String>	Read-write	Name of attribute15 that needs to be sent in SAML Assertion.
attribute15expr	<String>	Read-write	Expression that will be evaluated to obtain attribute15's value to be sent in Assertion. Maximum length = 128

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
attribute15friendlyname	<String>	Read-write	User-Friendly Name of attribute15 that needs to be sent in SAML Assertion.
attribute15format	<String>	Read-write	Format of Attribute15 to be sent in Assertion. Possible values = URI, Basic
attribute16	<String>	Read-write	Name of attribute16 that needs to be sent in SAML Assertion.
attribute16expr	<String>	Read-write	Expression that will be evaluated to obtain attribute16's value to be sent in Assertion. Maximum length = 128
attribute16friendlyname	<String>	Read-write	User-Friendly Name of attribute16 that needs to be sent in SAML Assertion.
attribute16format	<String>	Read-write	Format of Attribute16 to be sent in Assertion. Possible values = URI, Basic
encryptassertion	<String>	Read-write	Option to encrypt assertion when Citrix ADC sends one. Default value: OFF

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ON, OFF
samlspcertname	<String>	Read-write	Name of the SSL certificate of peer/ receving party using which Assertion is encrypted. Minimum length = 1
encryptionalgorithm	<String>	Read-write	Algorithm to be used to encrypt SAML assertion. Default value: AES256 Possible values = DES3, AES128, AES192, AES256
skewtime	<Integer>	Read-write	This option specifies the number of minutes on either side of current time that the assertion would be valid. For example, if skewTime is 10, then assertion would be valid from (current time - 10) min to (current time + 10) min, ie 20min in all. Default value: 5
signassertion	<String>	Read-write	Option to sign portions of assertion when Citrix ADC IDP sends one. Based on the user selection,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			either Assertion or Response or Both or none can be signed. Default value: ASSERTION Possible values = NONE, ASSERTION, RESPONSE, BOTH
signatureservice	<String>	Read-write	Name of the service in cloud used to sign the data. Minimum length = 1
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnsamlssoprofile **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"vpnsamlssoprofile":{

<b>"name":<String_value>,

</b>"samlsigningcertname":<String_value>,

<b>"assertionconsumerserviceurl":<String_value>,

</b>"relaystaterule":<String_value>,

"sendpassword":<String_value>,

"samlissuername":<String_value>,
```

```
"signaturealg":<String_value>,

"digestmethod":<String_value>,

"audience":<String_value>,

"nameidformat":<String_value>,

"nameidexpr":<String_value>,

"attribute1":<String_value>,

"attribute1expr":<String_value>,

"attribute1friendlyname":<String_value>,

"attribute1format":<String_value>,

"attribute2":<String_value>,

"attribute2expr":<String_value>,

"attribute2friendlyname":<String_value>,

"attribute2format":<String_value>,

"attribute3":<String_value>,

"attribute3expr":<String_value>,

"attribute3friendlyname":<String_value>,

"attribute3format":<String_value>,

"attribute4":<String_value>,

"attribute4expr":<String_value>,

"attribute4friendlyname":<String_value>,

"attribute4format":<String_value>,

"attribute5":<String_value>,
```

```
"attribute5expr":<String_value>,

"attribute5friendlyname":<String_value>,

"attribute5format":<String_value>,

"attribute6":<String_value>,

"attribute6expr":<String_value>,

"attribute6friendlyname":<String_value>,

"attribute6format":<String_value>,

"attribute7":<String_value>,

"attribute7expr":<String_value>,

"attribute7friendlyname":<String_value>,

"attribute7format":<String_value>,

"attribute8":<String_value>,

"attribute8expr":<String_value>,

"attribute8friendlyname":<String_value>,

"attribute8format":<String_value>,

"attribute9":<String_value>,

"attribute9expr":<String_value>,

"attribute9friendlyname":<String_value>,

"attribute9format":<String_value>,

"attribute10":<String_value>,

"attribute10expr":<String_value>,

"attribute10friendlyname":<String_value>,
```

```
"attribute10format":<String_value>,

"attribute11":<String_value>,

"attribute11expr":<String_value>,

"attribute11friendlyname":<String_value>,

"attribute11format":<String_value>,

"attribute12":<String_value>,

"attribute12expr":<String_value>,

"attribute12friendlyname":<String_value>,

"attribute12format":<String_value>,

"attribute13":<String_value>,

"attribute13expr":<String_value>,

"attribute13friendlyname":<String_value>,

"attribute13format":<String_value>,

"attribute14":<String_value>,

"attribute14expr":<String_value>,

"attribute14friendlyname":<String_value>,

"attribute14format":<String_value>,

"attribute15":<String_value>,

"attribute15expr":<String_value>,

"attribute15friendlyname":<String_value>,

"attribute15format":<String_value>,

"attribute16":<String_value>,
```

```
"attribute16expr":<String_value>,

"attribute16friendlyname":<String_value>,

"attribute16format":<String_value>,

"encryptassertion":<String_value>,

"samlspcertname":<String_value>,

"encryptionalgorithm":<String_value>,

"skewtime":<Integer_value>,

"signassertion":<String_value>,

"signatureservice":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnsamlssoprofile/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnsamlssoprofile **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"vpnsamlssoprofile":{

<b>"name":<String_value>,

</b>"samlsigningcertname":<String_value>,

"assertionconsumerserviceurl":<String_value>,

"sendpassword":<String_value>,

"samlissuername":<String_value>,

"relaystaterule":<String_value>,

"signaturealg":<String_value>,

"digestmethod":<String_value>,

"audience":<String_value>,

"nameidformat":<String_value>,

"nameidexpr":<String_value>,

"attribute1":<String_value>,

"attribute1expr":<String_value>,

"attribute1friendlyname":<String_value>,

"attribute1format":<String_value>,

"attribute2":<String_value>,

"attribute2expr":<String_value>,

"attribute2friendlyname":<String_value>,
```

```
"attribute2format":<String_value>,

"attribute3":<String_value>,

"attribute3expr":<String_value>,

"attribute3friendlyname":<String_value>,

"attribute3format":<String_value>,

"attribute4":<String_value>,

"attribute4expr":<String_value>,

"attribute4friendlyname":<String_value>,

"attribute4format":<String_value>,

"attribute5":<String_value>,

"attribute5expr":<String_value>,

"attribute5friendlyname":<String_value>,

"attribute5format":<String_value>,

"attribute6":<String_value>,

"attribute6expr":<String_value>,

"attribute6friendlyname":<String_value>,

"attribute6format":<String_value>,

"attribute7":<String_value>,

"attribute7expr":<String_value>,

"attribute7friendlyname":<String_value>,

"attribute7format":<String_value>,

"attribute8":<String_value>,
```

```
"attribute8expr":<String_value>,

"attribute8friendlyname":<String_value>,

"attribute8format":<String_value>,

"attribute9":<String_value>,

"attribute9expr":<String_value>,

"attribute9friendlyname":<String_value>,

"attribute9format":<String_value>,

"attribute10":<String_value>,

"attribute10expr":<String_value>,

"attribute10friendlyname":<String_value>,

"attribute10format":<String_value>,

"attribute11":<String_value>,

"attribute11expr":<String_value>,

"attribute11friendlyname":<String_value>,

"attribute11format":<String_value>,

"attribute12":<String_value>,

"attribute12expr":<String_value>,

"attribute12friendlyname":<String_value>,

"attribute12format":<String_value>,

"attribute13":<String_value>,

"attribute13expr":<String_value>,

"attribute13friendlyname":<String_value>,
```

```
"attribute13format":<String_value>,

"attribute14":<String_value>,

"attribute14expr":<String_value>,

"attribute14friendlyname":<String_value>,

"attribute14format":<String_value>,

"attribute15":<String_value>,

"attribute15expr":<String_value>,

"attribute15friendlyname":<String_value>,

"attribute15format":<String_value>,

"attribute16":<String_value>,

"attribute16expr":<String_value>,

"attribute16friendlyname":<String_value>,

"attribute16format":<String_value>,

"encryptassertion":<String_value>,

"samlspcertname":<String_value>,

"encryptionalgorithm":<String_value>,

"skewtime":<Integer_value>,

"signassertion":<String_value>,

"signatureservice":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnsamlssoprofile? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"vpnsamlssoprofile":{

<b>"name":<String_value>,

</b>"samlsigningcertname":true,

"sendpassword":true,

"samlissuername":true,

"relaystaterule":true,

"signaturealg":true,

"digestmethod":true,

"audience":true,

"nameidformat":true,

"nameidexpr":true,

"attribute1":true,

"attribute1friendlyname":true,

"attribute1format":true,
```

```
"attribute2":true,
"attribute2friendlyname":true,
"attribute2format":true,
"attribute3":true,
"attribute3friendlyname":true,
"attribute3format":true,
"attribute4":true,
"attribute4friendlyname":true,
"attribute4format":true,
"attribute5":true,
"attribute5friendlyname":true,
"attribute5format":true,
"attribute6":true,
"attribute6friendlyname":true,
"attribute6format":true,
"attribute7":true,
"attribute7friendlyname":true,
"attribute7format":true,
"attribute8":true,
"attribute8friendlyname":true,
"attribute8format":true,
"attribute9":true,
```

```
"attribute9friendlyname":true,

"attribute9format":true,

"attribute10":true,

"attribute10friendlyname":true,

"attribute10format":true,

"attribute11":true,

"attribute11friendlyname":true,

"attribute11format":true,

"attribute12":true,

"attribute12friendlyname":true,

"attribute12format":true,

"attribute13":true,

"attribute13friendlyname":true,

"attribute13format":true,

"attribute14":true,

"attribute14friendlyname":true,

"attribute14format":true,

"attribute15":true,

"attribute15friendlyname":true,

"attribute15format":true,

"attribute16":true,

"attribute16friendlyname":true,
```

```
"attribute16format":true,

"encryptassertion":true,

"samlspcertname":true,

"encryptionalgorithm":true,

"skewtime":true,

"signassertion":true,

"signatureservice":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnsamlssoprofile **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/vpnsamlssoprofile? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/vpnsamlssoprofile? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of vpnsamlssoprofile resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/vpnsamlssoprofile? **view=summary**

Use this query-parameter to get the summary output of vpnsamlssoprofile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/vpnsamlssoprofile? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vpnsamlssoprofile resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vpnsamlssoprofile": [ {

"name":<String_value>,

"samlsigningcertname":<String_value>,

"assertionconsumerserviceurl":<String_value>,

"sendpassword":<String_value>,

"samlissuername":<String_value>,

"relaystaterule":<String_value>,

"signaturealg":<String_value>,

"digestmethod":<String_value>,

"audience":<String_value>,
```

```
"nameidformat":<String_value>,

"nameidexpr":<String_value>,

"attribute1":<String_value>,

"attribute2":<String_value>,

"attribute3":<String_value>,

"attribute4":<String_value>,

"attribute5":<String_value>,

"attribute6":<String_value>,

"attribute7":<String_value>,

"attribute8":<String_value>,

"attribute9":<String_value>,

"attribute10":<String_value>,

"attribute11":<String_value>,

"attribute12":<String_value>,

"attribute13":<String_value>,

"attribute14":<String_value>,

"attribute15":<String_value>,

"attribute16":<String_value>,

"attribute1friendlyname":<String_value>,

"attribute2friendlyname":<String_value>,

"attribute3friendlyname":<String_value>,

"attribute4friendlyname":<String_value>,
```

```
"attribute5friendlyname":<String_value>,

"attribute6friendlyname":<String_value>,

"attribute7friendlyname":<String_value>,

"attribute8friendlyname":<String_value>,

"attribute9friendlyname":<String_value>,

"attribute10friendlyname":<String_value>,

"attribute11friendlyname":<String_value>,

"attribute12friendlyname":<String_value>,

"attribute13friendlyname":<String_value>,

"attribute14friendlyname":<String_value>,

"attribute15friendlyname":<String_value>,

"attribute16friendlyname":<String_value>,

"attribute1format":<String_value>,

"attribute2format":<String_value>,

"attribute3format":<String_value>,

"attribute4format":<String_value>,

"attribute5format":<String_value>,

"attribute6format":<String_value>,

"attribute7format":<String_value>,

"attribute8format":<String_value>,

"attribute9format":<String_value>,

"attribute10format":<String_value>,
```

```
"attribute11format":<String_value>,

"attribute12format":<String_value>,

"attribute13format":<String_value>,

"attribute14format":<String_value>,

"attribute15format":<String_value>,

"attribute16format":<String_value>,

"attribute1expr":<String_value>,

"attribute2expr":<String_value>,

"attribute3expr":<String_value>,

"attribute4expr":<String_value>,

"attribute5expr":<String_value>,

"attribute6expr":<String_value>,

"attribute7expr":<String_value>,

"attribute8expr":<String_value>,

"attribute9expr":<String_value>,

"attribute10expr":<String_value>,

"attribute11expr":<String_value>,

"attribute12expr":<String_value>,

"attribute13expr":<String_value>,

"attribute14expr":<String_value>,

"attribute15expr":<String_value>,

"attribute16expr":<String_value>,
```

```
"encryptassertion":<String_value>,

"samlspcertname":<String_value>,

"encryptionalgorithm":<String_value>,

"skewtime":<Integer_value>,

"signassertion":<String_value>,

"signatureservice":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnsamlssoprofile/ name_value<String>
Query-parameters: attrs http:// <netscaler-ip-address> /nitro/v1/config/vpnsamlssoprofile/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/vpnsamlssoprofile/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of vpnsamlssoprofile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnsamlssoprofile": [ {

"name":<String_value>,

"samlsigningcertname":<String_value>,

"assertionconsumerserviceurl":<String_value>,

"sendpassword":<String_value>,

"samlissuername":<String_value>,

"relaystaterule":<String_value>,

"signaturealg":<String_value>,

"digestmethod":<String_value>,

"audience":<String_value>,

"nameidformat":<String_value>,

"nameidexpr":<String_value>,

"attribute1":<String_value>,

"attribute2":<String_value>,

"attribute3":<String_value>,

"attribute4":<String_value>,

"attribute5":<String_value>,
```

```
"attribute6":<String_value>,

"attribute7":<String_value>,

"attribute8":<String_value>,

"attribute9":<String_value>,

"attribute10":<String_value>,

"attribute11":<String_value>,

"attribute12":<String_value>,

"attribute13":<String_value>,

"attribute14":<String_value>,

"attribute15":<String_value>,

"attribute16":<String_value>,

"attribute1friendlyname":<String_value>,

"attribute2friendlyname":<String_value>,

"attribute3friendlyname":<String_value>,

"attribute4friendlyname":<String_value>,

"attribute5friendlyname":<String_value>,

"attribute6friendlyname":<String_value>,

"attribute7friendlyname":<String_value>,

"attribute8friendlyname":<String_value>,

"attribute9friendlyname":<String_value>,

"attribute10friendlyname":<String_value>,

"attribute11friendlyname":<String_value>,
```

```
"attribute12friendlyname":<String_value>,

"attribute13friendlyname":<String_value>,

"attribute14friendlyname":<String_value>,

"attribute15friendlyname":<String_value>,

"attribute16friendlyname":<String_value>,

"attribute1format":<String_value>,

"attribute2format":<String_value>,

"attribute3format":<String_value>,

"attribute4format":<String_value>,

"attribute5format":<String_value>,

"attribute6format":<String_value>,

"attribute7format":<String_value>,

"attribute8format":<String_value>,

"attribute9format":<String_value>,

"attribute10format":<String_value>,

"attribute11format":<String_value>,

"attribute12format":<String_value>,

"attribute13format":<String_value>,

"attribute14format":<String_value>,

"attribute15format":<String_value>,

"attribute16format":<String_value>,

"attribute1expr":<String_value>,
```

```
"attribute2expr":<String_value>,

"attribute3expr":<String_value>,

"attribute4expr":<String_value>,

"attribute5expr":<String_value>,

"attribute6expr":<String_value>,

"attribute7expr":<String_value>,

"attribute8expr":<String_value>,

"attribute9expr":<String_value>,

"attribute10expr":<String_value>,

"attribute11expr":<String_value>,

"attribute12expr":<String_value>,

"attribute13expr":<String_value>,

"attribute14expr":<String_value>,

"attribute15expr":<String_value>,

"attribute16expr":<String_value>,

"encryptassertion":<String_value>,

"samlspcertname":<String_value>,

"encryptionalgorithm":<String_value>,

"skewtime":<Integer_value>,

"signassertion":<String_value>,

"signatureservice":<String_value>,

"_nextgenapiresource":<String_value>
```

```
}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnsamlssoprofile? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vpnsamlssoprofile": [ { "__count": "#no"} ] }
```

vpnsecureprivateaccessprofile

Configuration for Secure Private Access Profile resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	name of Secure Private Access profile. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum length = 31
url	<String>	Read-write	Public URL for your Secure Private Access site or load balancing server.
customerid	<String>	Read-write	Customer ID of the citrix cloud customer. Minimum length = 1
chromeenterprisepremiummode	<String>	Read-write	Secure Private Access Chrome Enterprise Premium mode of operation. Default value: OFF Possible values = OFF, WITH_PARTNER_CONNECTOR, WITHOUT_PARTNER_CONNECTOR
googlecustomerid	<String>	Read-write	Your organization's unique ID on Google's Admin console Profile settings. Minimum length = 1
googlesecuritygatewayid	<String>	Read-write	The ID of the Google Secure Gateway. Minimum length = 1
forceclienttype	<String>	Read-write	Automatically configures the session for Citrix

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Secure Access client connectivity. Default value: ON Possible values = ON, OFF
sharedsecret	<String>	Read-write	Secure Private Access Shared Secret. Minimum length = 32
clouddeployment	<String>	Read-only	Secure Private Access cloud deployment. Default value: PRODUCTION Possible values = PRODUCTION, STAGING, DEVELOPMENT
accessrestrictedpage redirect	<String>	Read-only	Redirect option for access restricted pages. Default value: CDN Possible values = CDN, NS, OFF
serverstatus	<String>	Read-only	Status of the Secure Private Access site as determined by a TCP monitor health check. Possible values = UP, DOWN

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnsecureprivateaccessprofile **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"vpnsecureprivateaccessprofile":{

<b>"name":<String_value>,

</b><b>"url":<String_value>,

</b>"customerid":<String_value>,

"chromeenterprisepremiummode":<String_value>,

"googlecustomerid":<String_value>,

"googlesecuritygatewayid":<String_value>,

"forceclienttype":<String_value>,

"sharedsecret":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnsecureprivateaccessprofile/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnsecureprivateaccessprofile **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"vpnsecureprivateaccessprofile":{

<b>"name":<String_value>,

</b>"url":<String_value>,

"customerid":<String_value>,

"chromeenterprisepremiummode":<String_value>,

"googlecustomerid":<String_value>,

"googlesecuritygatewayid":<String_value>,

"forceclienttype":<String_value>,

"sharedsecret":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnsecureprivateaccessprofile? **action=unset**
HTTP Method: POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"vpnsecureprivateaccessprofile":{

<b>"name":<String_value>,

</b>"customerid":true,

"chromeenterprisepremiummode":true,

"googlecustomerid":true,

"googlesecuritygatewayid":true,

"forceclienttype":true,

"sharedsecret":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnsecureprivateaccessprofile **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/vpnsecureprivateaccessprofile?**attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/vpnsecureprivateaccessprofile?**filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of vpnsecureprivateaccessprofile resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/vpnsecureprivateaccessprofile?**view=summary**

Use this query-parameter to get the summary output of vpnsecureprivateaccessprofile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/vpnsecureprivateaccessprofile?**pagesize=#no;pageno=#no**

Use this query-parameter to get the vpnsecureprivateaccessprofile resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vpnsecureprivateaccessprofile": [ {

"name":<String_value>,

"url":<String_value>,

"clouddeployment":<String_value>,

"customerid":<String_value>,

"accessrestrictedpageredirect":<String_value>,

"chromeenterprisepremiummode":<String_value>,

"googlecustomerid":<String_value>,

"forceclienttype":<String_value>,

"googlesecuritygatewayid":<String_value>,

"sharedsecret":<String_value>,

"serverstatus":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnsecureprivateaccessprofile/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/ vpnsecureprivateaccessprofile/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/vpnsecureprivateaccessprofile/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of vpnsecureprivateaccessprofile resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnsecureprivateaccessprofile": [ {

"name":<String_value>,

"url":<String_value>,

"clouddeployment":<String_value>,

"customerid":<String_value>,

"accessrestrictedpageredirect":<String_value>,

"chromeenterprisepremiummode":<String_value>,

"googlecustomerid":<String_value>,

"forceclienttype":<String_value>,

"googlesecuritygatewayid":<String_value>,

"sharedsecret":<String_value>,

"serverstatus":<String_value>,
```

```
"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnsecureprivateaccessprofile? **count=yes**
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vpnsecureprivateaccessprofile": [ { "__count": "#no"} ] }
```

vpnsessionaction

Configuration for VPN session action resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the Citrix Gateway profile (action). Must begin with an ASCII

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			alphabetic or underscore (_) character, and must consist only of ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the profile is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my action" or 'my action'). Minimum length = 1
useraccounting	<String>	Read-write	The name of the radiusPolicy to use for RADIUS user accounting info on the session.
httpport	<Integer[]>	Read-write	Destination port numbers other than port 80, added as a comma-separated list. Traffic to these

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			ports is processed as HTTP traffic, which allows functionality, such as HTTP authorization and single sign-on to a web application to work. Minimum value = 1
winsip	<String>	Read-write	WINS server IP address to add to Citrix Gateway for name resolution.
dnsvservername	<String>	Read-write	Name of the DNS virtual server for the user session. Minimum length = 1
splitdns	<String>	Read-write	Route the DNS requests to the local DNS server configured on the user device, or Citrix Gateway (remote), or both. Possible values = LOCAL, REMOTE, BOTH
sesstimeout	<Integer>	Read-write	Number of minutes after which the session times out. Minimum value = 1
clientsecurity	<String>	Read-write	Specify the client security check for the user device to permit a Citrix Gateway session. The web

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			address or IP address is not included in the expression for the client security check.
clientsecuritygroup	<String>	Read-write	The client security group that will be assigned on failure of the client security check. Users can in general be organized into Groups. In this case, the Client Security Group may have a more restrictive security policy. Minimum length = 1
clientsecuritymessage	<String>	Read-write	The client security message that will be displayed on failure of the client security check. Minimum length = 1 Maximum length = 127
clientsecuritylog	<String>	Read-write	Set the logging of client security checks. Possible values = ON, OFF
splittunnel	<String>	Read-write	Send, through the tunnel, traffic only for intranet applications that are defined in Citrix Gateway.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Route all other traffic directly to the Internet. The OFF setting routes all traffic through Citrix Gateway. With the REVERSE setting, intranet applications define the network traffic that is not intercepted. All network traffic directed to internal IP addresses bypasses the VPN tunnel, while other traffic goes through Citrix Gateway. Reverse split tunneling can be used to log all non-local LAN traffic. For example, if users have a home network and are logged on through the Citrix Gateway Plug-in, network traffic destined to a printer or another device within the home network is not intercepted. Possible values = ON, OFF, REVERSE
locallanaccess	<String>	Read-write	Set local LAN access. If split tunneling is OFF, and you set local LAN access to ON, the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			local client can route traffic to its local interface. When the local area network switch is specified, this combination of switches is useful. The client can allow local LAN access to devices that commonly have non-routable addresses, such as local printers or local file servers. Possible values = ON, OFF, FORCED
rfc1918	<String>	Read-write	As defined in the local area network, allow only the following local area network addresses to bypass the VPN tunnel when the local LAN access feature is enabled: * 10.*.*.*, * 172.16.*.*, * 192.168.*.*. Possible values = ON, OFF
spoofiip	<String>	Read-write	IP address that the intranet application uses to route the connection through the virtual adapter.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ON, OFF
killconnections	<String>	Read-write	Specify whether the Citrix Gateway Plug-in should disconnect all preexisting connections, such as the connections existing before the user logged on to Citrix Gateway, and prevent new incoming connections on the Citrix Gateway Plug-in for Windows and MAC when the user is connected to Citrix Gateway and split tunneling is disabled. Possible values = ON, OFF
transparentintercepti on	<String>	Read-write	Allow access to network resources by using a single IP address and subnet mask or a range of IP addresses. The OFF setting sets the mode to proxy, in which you configure destination and source IP addresses and port numbers. If you are using the Citrix Gateway Plug-in for Windows, set this parameter to ON, in which the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			mode is set to transparent. If you are using the Citrix Gateway Plug-in for Java, set this parameter to OFF. Possible values = ON, OFF
windowsclienttype	<String>	Read-write	Choose between two types of Windows Client\ a) Application Agent - which always runs in the task bar as a standalone application and also has a supporting service which runs permanently when installed b) Activex Control - ActiveX control run by Microsoft Internet Explorer. Possible values = AGENT, PLUGIN
defaultauthorizationaction	<String>	Read-write	Specify the network resources that users have access to when they log on to the internal network. The default setting for authorization is to deny access to all network resources.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Citrix recommends using the default global setting and then creating authorization policies to define the network resources users can access. If you set the default authorization policy to DENY, you must explicitly authorize access to any network resource, which improves security. Possible values = ALLOW, DENY
authorizationgroup	<String>	Read-write	Comma-separated list of groups in which the user is placed when none of the groups that the user is a part of is configured on Citrix Gateway. The authorization policy can be bound to these groups to control access to the resources. Minimum length = 1
smartgroup	<String>	Read-write	This is the default group that is chosen when the authentication succeeds in addition to extracted groups. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum length = 64
clientidletimeout	<Integer>	Read-write	Time, in minutes, after which to time out the user session if Citrix Gateway does not detect mouse or keyboard activity. Minimum value = 1 Maximum value = 9999
proxy	<String>	Read-write	Set options to apply proxy for accessing the internal resources. Available settings function as follows: * BROWSER - Proxy settings are configured only in Internet Explorer and Firefox browsers. * NS - Proxy settings are configured on the Citrix ADC. * OFF - Proxy settings are not configured.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = BROWSER, NS, OFF
allprotocolproxy	<String>	Read-write	IP address of the proxy server to use for all protocols supported by Citrix Gateway. Minimum length = 1
httpproxy	<String>	Read-write	IP address of the proxy server to be used for HTTP access for all subsequent connections to the internal network. Minimum length = 1
ftpproxy	<String>	Read-write	IP address of the proxy server to be used for FTP access for all subsequent connections to the internal network. Minimum length = 1
socksproxy	<String>	Read-write	IP address of the proxy server to be used for SOCKS access for all subsequent connections to the internal network. Minimum length = 1
gopherproxy	<String>	Read-write	IP address of the proxy server to be used for GOPHER access for all

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			subsequent connections to the internal network. Minimum length = 1
sslproxy	<String>	Read-write	IP address of the proxy server to be used for SSL access for all subsequent connections to the internal network. Minimum length = 1
proxyexception	<String>	Read-write	Proxy exception string that will be configured in the browser for bypassing the previously configured proxies. Allowed only if proxy type is Browser. Minimum length = 1
proxylocalbypass	<String>	Read-write	Bypass proxy server for local addresses option in Internet Explorer and Firefox proxy server settings. Possible values = ENABLED, DISABLED
clientcleanupprompt	<String>	Read-write	Prompt for client-side cache clean-up when a client-initiated session closes. Possible values = ON, OFF

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
forcecleanup	<String[]>	Read-write	Force cache clean-up when the user closes a session. You can specify all, none, or any combination of the client-side items. Possible values = none, all, cookie, addressbar, plugin, filesystemapplicatio n, application, applicationdata, clientcertificate, autocomplete, cache
clientoptions	<String>	Read-write	Display only the configured menu options when you select the "Configure Citrix Gateway" option in the Citrix Gateway Plug-in system tray icon for Windows. Possible values = none, all, services, filetransfer, configuration
clientconfiguration	<String[]>	Read-write	Allow users to change client Debug logging level in Configuration tab of the Citrix Gateway Plug-in for Windows.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = none, trace
sso	<String>	Read-write	Set single sign-on (SSO) for the session. When the user accesses a server, the user's logon credentials are passed to the server for authentication. NOTE : This configuration does not honor the following authentication types for security reason. BASIC, DIGEST, and NTLM (without Negotiate NTLM2 Key or Negotiate Sign Flag). Use VPN TrafficAction to configure SSO for these authentication types. Possible values = ON, OFF
ssocredential	<String>	Read-write	Specify whether to use the primary or secondary authentication credentials for single sign-on to the server.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = PRIMARY, SECONDARY
windowsautologon	<String>	Read-write	Enable or disable the Windows Auto Logon for the session. If a VPN session is established after this setting is enabled, the user is automatically logged on by using Windows credentials after the system is restarted. Possible values = ON, OFF
usemip	<String>	Read-write	Enable or disable the use of a unique IP address alias, or a mapped IP address, as the client IP address for each client session. Allow Citrix Gateway to use the mapped IP address as an intranet IP address when all other IP addresses are not available. When IP pooling is configured and the mapped IP is used as an intranet IP address, the mapped IP address is used when an

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			intranet IP address cannot be assigned. Possible values = NS, OFF
useiip	<String>	Read-write	Define IP address pool options. Available settings function as follows: * SPILLOVER - When an address pool is configured and the mapped IP is used as an intranet IP address, the mapped IP address is used when an intranet IP address cannot be assigned. * NOSPILLOVER - When intranet IP addresses are enabled and the mapped IP address is not used, the Transfer Login page appears for users who have used all available intranet IP addresses. * OFF - Address pool is not configured.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = NOSPILLOVER, SPILLOVER, OFF
clientdebug	<String>	Read-write	Set the trace level on Citrix Gateway. Technical support technicians use these debug logs for in-depth debugging and troubleshooting purposes. Available settings function as follows: * DEBUG - Detailed debug messages are collected and written into the specified file. * STATS - Application audit level error messages and debug statistic counters are written into the specified file. * EVENTS - Application audit-level error messages are written into the specified file. * OFF - Only critical events are logged

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			into the Windows Application Log. Possible values = debug, stats, events, OFF
loginscript	<String>	Read-write	Path to the logon script that is run when a session is established. Separate multiple scripts by using comma. A "$" in the path signifies that the word following the "$" is an environment variable. Minimum length = 1
logoutscript	<String>	Read-write	Path to the logout script. Separate multiple scripts by using comma. A "$" in the path signifies that the word following the "$" is an environment variable. Minimum length = 1
homepage	<String>	Read-write	Web address of the home page that appears when users log on. Otherwise, users receive the default home page for Citrix Gateway, which is the Access Interface.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
icaproxy	<String>	Read-write	Enable ICA proxy to configure secure Internet access to servers running Citrix XenApp or XenDesktop by using Citrix Receiver instead of the Citrix Gateway Plug-in. Possible values = ON, OFF
wihome	<String>	Read-write	Web address of the Web Interface server, such as http://<ipAddress>/Citrix/XenApp, or Receiver for Web, which enumerates the virtualized resources, such as XenApp, XenDesktop, and cloud applications. This web address is used as the home page in ICA proxy mode. If Client Choices is ON, you must configure this setting. Because the user can choose between FullClient and ICAProxy, the user may see a different home page. An Internet web site may

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			appear if the user gets the FullClient option, or a Web Interface site if the user gets the ICAProxy option. If the setting is not configured, the XenApp option does not appear as a client choice.
wihomeaddresstype	<String>	Read-write	Type of the wihome address(IPV4/V6). Possible values = IPV4, IPV6
citrixreceiverhome	<String>	Read-write	Web address for the Citrix Receiver home page. Configure Citrix Gateway so that when users log on to the appliance, the Citrix Gateway Plug-in opens a web browser that allows single sign-on to the Citrix Receiver home page.
wiportalmode	<String>	Read-write	Layout on the Access Interface. The COMPACT value indicates the use of small icons. Possible values = NORMAL, COMPACT

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
clientchoices	<String>	Read-write	Provide users with multiple logon options. With client choices, users have the option of logging on by using the Citrix Gateway Plug-in for Windows, Citrix Gateway Plug-in for Java, the Web Interface, or clientless access from one location. Depending on how Citrix Gateway is configured, users are presented with up to three icons for logon choices. The most common are the Citrix Gateway Plug-in for Windows, Web Interface, and clientless access. Possible values = ON, OFF
epaclienttype	<String>	Read-write	Choose between two types of End point Windows Client a) Application Agent - which always runs in the task bar as a standalone application and also has a supporting service which runs

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			permanently when installed b) Activex Control - ActiveX control run by Microsoft Internet Explorer. Possible values = AGENT, PLUGIN
iipdnssuffix	<String>	Read-write	An intranet IP DNS suffix. When a user logs on to Citrix Gateway and is assigned an IP address, a DNS record for the user name and IP address combination is added to the Citrix Gateway DNS cache. You can configure a DNS suffix to append to the user name when the DNS record is added to the cache. You can reach to the host from where the user is logged on by using the user's name, which can be easier to remember than an IP address. When the user logs off from Citrix Gateway, the record is removed from the DNS cache.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum length = 1
forcedtimeout	<Integer>	Read-write	Force a disconnection from the Citrix Gateway Plug-in with Citrix Gateway after a specified number of minutes. If the session closes, the user must log on again. Minimum value = 1 Maximum value = 65535
forcedtimeoutwarning	<Integer>	Read-write	Number of minutes to warn a user before the user session is disconnected. Minimum value = 1 Maximum value = 255
ntdomain	<String>	Read-write	Single sign-on domain to use for single sign-on to applications in the internal network. This setting can be overwritten by the domain that users specify at the time of logon or by the domain that the authentication server returns. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum length = 32
clientlessvpnmode	<String>	Read-write	Enable clientless access for web, XenApp or XenDesktop, and FileShare resources without installing the Citrix Gateway Plug-in. Available settings function as follows: * ON - Allow only clientless access. * OFF - Allow clientless access after users log on with the Citrix Gateway Plug-in. * DISABLED - Do not allow clientless access. Possible values = ON, OFF, DISABLED
emailhome	<String>	Read-write	Web address for the web-based email, such as Outlook Web Access.
clientlessmodeurlencoding	<String>	Read-write	When clientless access is enabled, you can choose to encode the addresses of internal web applications or

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			to leave the address as clear text. Available settings function as follows: * OPAQUE - Use standard encoding mechanisms to make the domain and protocol part of the resource unclear to users. * CLEAR - Do not encode the web address and make it visible to users. * ENCRYPT - Allow the domain and protocol to be encrypted using a session key. When the web address is encrypted, the URL is different for each user session for the same web resource. If users bookmark the encoded web address, save it in the web browser and then log off, they cannot connect to the web address when they log on and use the bookmark. If users

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			save the encrypted bookmark in the Access Interface during their session, the bookmark works each time the user logs on. Possible values = TRANSPARENT, OPAQUE, ENCRYPT
clientlesspersistentcookie	<String>	Read-write	State of persistent cookies in clientless access mode. Persistent cookies are required for accessing certain features of SharePoint, such as opening and editing Microsoft Word, Excel, and PowerPoint documents hosted on the SharePoint server. A persistent cookie remains on the user device and is sent with each HTTP request. Citrix Gateway encrypts the persistent cookie before sending it to the plug-in on the user device, and refreshes the cookie periodically as long as the session

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			exists. The cookie becomes stale if the session ends. Available settings function as follows: * ALLOW - Enable persistent cookies. Users can open and edit Microsoft documents stored in SharePoint. * DENY - Disable persistent cookies. Users cannot open and edit Microsoft documents stored in SharePoint. * PROMPT - Prompt users to allow or deny persistent cookies during the session. Persistent cookies are not required for clientless access if users do not connect to SharePoint. Possible values = ALLOW, DENY, PROMPT
allowedlogingroups	<String>	Read-write	Specify groups that have permission to log on to Citrix

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Gateway. Users who do not belong to this group or groups are denied access even if they have valid credentials. Minimum length = 1 Maximum length = 511
securebrowse	<String>	Read-write	Allow users to connect through Citrix Gateway to network resources from iOS and Android mobile devices with Citrix Receiver. Users do not need to establish a full VPN tunnel to access resources in the secure network. Possible values = ENABLED, DISABLED
storefronturl	<String>	Read-write	Web address for StoreFront to be used in this session for enumeration of resources from XenApp or XenDesktop. Minimum length = 1 Maximum length = 255

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
sfgatewayauthtype	<String>	Read-write	The authentication type configured for the Citrix Gateway on StoreFront. Possible values = domain, RSA, domainAndRSA, SMS, smartCard, sfAuth, sfAuthAndRSA
kcdaccount	<String>	Read-write	The kcd account details to be used in SSO. Minimum length = 1 Maximum length = 32
rdpclientprofilename	<String>	Read-write	Name of the RDP profile associated with the vserver. Minimum length = 1 Maximum length = 31
windowspluginupgrade	<String>	Read-write	Option to set plugin upgrade behaviour for Win. Possible values = Always, Essential, Never
macpluginupgrade	<String>	Read-write	Option to set plugin upgrade behaviour for Mac.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = Always, Essential, Never
linuxpluginupgrade	<String>	Read-write	Option to set plugin upgrade behaviour for Linux. Possible values = Always, Essential, Never
iconwithreceiver	<String>	Read-write	Option to decide whether to show plugin icon along with receiver. Possible values = ON, OFF
alwaysonprofilename	<String>	Read-write	Name of the AlwaysON profile associated with the session action. The builtin profile named none can be used to explicitly disable AlwaysON for the session action. Minimum length = 1 Maximum length = 31
autoproxyurl	<String>	Read-write	URL to auto proxy config file.
advancedclientlessvpnmode	<String>	Read-write	Option to enable/disable Advanced ClientlessVpnMode. Additionaly, it can be set to STRICT to

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			block Classic ClientlessVpnMode while in AdvancedClientless Mode. Default value: DISABLED Possible values = ENABLED, DISABLED, STRICT
pcoipprofilename	<String>	Read-write	Name of the PCOIP profile associated with the session action. The builtin profile named none can be used to explicitly disable PCOIP for the session action. Minimum length = 1 Maximum length = 31
fqdnspoofedip	<String>	Read-write	Spoofed IP address range that can be used by client for FQDN based split tunneling. Minimum length = 1
netmask	<String>	Read-write	The netmask for the spoofed ip address. Minimum length = 1
clientidletimeoutwarning	<Integer>	Read-only	The time after which the client gets a

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			timeout warning, in minutes.
builtin	<String[]>	Read-only	Indicates that a variable is a built-in (SYSTEM INTERNAL) type. Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL
feature	<String>	Read-only	The feature to be checked while applying this config.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnsessionaction **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"vpnsessionaction":{

<b>"name":<String_value>,

</b>"useraccounting":<String_value>,

"httpport":<Integer[]_value>,

"winsip":<String_value>,

"dnsvservername":<String_value>,
```

```
"splitdns":<String_value>,

"sesstimeout":<Integer_value>,

"clientsecurity":<String_value>,

"clientsecuritygroup":<String_value>,

"clientsecuritymessage":<String_value>,

"clientsecuritylog":<String_value>,

"splittunnel":<String_value>,

"locallanaccess":<String_value>,

"rfc1918":<String_value>,

"spoofiip":<String_value>,

"killconnections":<String_value>,

"transparentinterception":<String_value>,

"windowsclienttype":<String_value>,

"defaultauthorizationaction":<String_value>,

"authorizationgroup":<String_value>,

"smartgroup":<String_value>,

"clientidletimeout":<Integer_value>,

"proxy":<String_value>,

"allprotocolproxy":<String_value>,

"httpproxy":<String_value>,

"ftpproxy":<String_value>,

"socksproxy":<String_value>,
```

```
"gopherproxy":<String_value>,

"sslproxy":<String_value>,

"proxyexception":<String_value>,

"proxylocalbypass":<String_value>,

"clientcleanupprompt":<String_value>,

"forcecleanup":<String[]_value>,

"clientoptions":<String_value>,

"clientconfiguration":<String[]_value>,

"sso":<String_value>,

"ssocredential":<String_value>,

"windowsautologon":<String_value>,

"usemip":<String_value>,

"useiip":<String_value>,

"clientdebug":<String_value>,

"loginscript":<String_value>,

"logoutscript":<String_value>,

"homepage":<String_value>,

"icaproxy":<String_value>,

"wihome":<String_value>,

"wihomeaddresstype":<String_value>,

"citrixreceiverhome":<String_value>,

"wiportalmode":<String_value>,
```

```
"clientchoices":<String_value>,

"epaclienttype":<String_value>,

"iipdnssuffix":<String_value>,

"forcedtimeout":<Integer_value>,

"forcedtimeoutwarning":<Integer_value>,

"ntdomain":<String_value>,

"clientlessvpnmode":<String_value>,

"emailhome":<String_value>,

"clientlessmodeurlencoding":<String_value>,

"clientlesspersistentcookie":<String_value>,

"allowedlogingroups":<String_value>,

"securebrowse":<String_value>,

"storefronturl":<String_value>,

"sfgatewayauthtype":<String_value>,

"kcdaccount":<String_value>,

"rdpclientprofilename":<String_value>,

"windowspluginupgrade":<String_value>,

"macpluginupgrade":<String_value>,

"linuxpluginupgrade":<String_value>,

"iconwithreceiver":<String_value>,

"alwaysonprofilename":<String_value>,

"autoproxyurl":<String_value>,
```

```
"advancedclientlessvpnmode":<String_value>,

"pcoipprofilename":<String_value>,

"fqdnspoofedip":<String_value>,

"netmask":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnsessionaction/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnsessionaction **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"vpnsessionaction":{

<b>"name":<String_value>,
```

```
</b>"useraccounting":<String_value>,

"httpport":<Integer[]_value>,

"winsip":<String_value>,

"dnsvservername":<String_value>,

"splitdns":<String_value>,

"sesstimeout":<Integer_value>,

"clientsecurity":<String_value>,

"clientsecuritygroup":<String_value>,

"clientsecuritymessage":<String_value>,

"clientsecuritylog":<String_value>,

"splittunnel":<String_value>,

"locallanaccess":<String_value>,

"rfc1918":<String_value>,

"spoofiip":<String_value>,

"killconnections":<String_value>,

"transparentinterception":<String_value>,

"windowsclienttype":<String_value>,

"defaultauthorizationaction":<String_value>,

"authorizationgroup":<String_value>,

"smartgroup":<String_value>,

"clientidletimeout":<Integer_value>,

"proxy":<String_value>,
```

```
"allprotocolproxy":<String_value>,

"httpproxy":<String_value>,

"ftpproxy":<String_value>,

"socksproxy":<String_value>,

"gopherproxy":<String_value>,

"sslproxy":<String_value>,

"proxyexception":<String_value>,

"proxylocalbypass":<String_value>,

"clientcleanupprompt":<String_value>,

"forcecleanup":<String[]_value>,

"clientoptions":<String_value>,

"clientconfiguration":<String[]_value>,

"sso":<String_value>,

"ssocredential":<String_value>,

"windowsautologon":<String_value>,

"usemip":<String_value>,

"useiip":<String_value>,

"clientdebug":<String_value>,

"loginscript":<String_value>,

"logoutscript":<String_value>,

"homepage":<String_value>,

"icaproxy":<String_value>,
```

```
"wihome":<String_value>,

"wihomeaddresstype":<String_value>,

"citrixreceiverhome":<String_value>,

"wiportalmode":<String_value>,

"clientchoices":<String_value>,

"epaclienttype":<String_value>,

"iipdnssuffix":<String_value>,

"forcedtimeout":<Integer_value>,

"forcedtimeoutwarning":<Integer_value>,

"ntdomain":<String_value>,

"clientlessvpnmode":<String_value>,

"emailhome":<String_value>,

"clientlessmodeurlencoding":<String_value>,

"clientlesspersistentcookie":<String_value>,

"allowedlogingroups":<String_value>,

"securebrowse":<String_value>,

"storefronturl":<String_value>,

"sfgatewayauthtype":<String_value>,

"kcdaccount":<String_value>,

"rdpclientprofilename":<String_value>,

"windowspluginupgrade":<String_value>,

"macpluginupgrade":<String_value>,
```

```
"linuxpluginupgrade":<String_value>,

"iconwithreceiver":<String_value>,

"alwaysonprofilename":<String_value>,

"autoproxyurl":<String_value>,

"advancedclientlessvpnmode":<String_value>,

"pcoipprofilename":<String_value>,

"fqdnspoofedip":<String_value>,

"netmask":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnsessionaction? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"vpnsessionaction":{

<b>"name":<String_value>,

</b>"useraccounting":true,
```

```
"httpport":true,

"winsip":true,

"dnsvservername":true,

"splitdns":true,

"sesstimeout":true,

"clientsecurity":true,

"clientsecuritygroup":true,

"clientsecuritymessage":true,

"clientsecuritylog":true,

"splittunnel":true,

"locallanaccess":true,

"rfc1918":true,

"spoofiip":true,

"killconnections":true,

"transparentinterception":true,

"windowsclienttype":true,

"defaultauthorizationaction":true,

"authorizationgroup":true,

"smartgroup":true,

"clientidletimeout":true,

"proxy":true,

"allprotocolproxy":true,
```

```
"httpproxy":true,

"ftpproxy":true,

"socksproxy":true,

"gopherproxy":true,

"sslproxy":true,

"proxyexception":true,

"proxylocalbypass":true,

"clientcleanupprompt":true,

"forcecleanup":true,

"clientoptions":true,

"clientconfiguration":true,

"sso":true,

"ssocredential":true,

"windowsautologon":true,

"usemip":true,

"useiip":true,

"clientdebug":true,

"loginscript":true,

"logoutscript":true,

"homepage":true,

"icaproxy":true,

"wihome":true,
```

```
"citrixreceiverhome":true,

"wiportalmode":true,

"clientchoices":true,

"epaclienttype":true,

"iipdnssuffix":true,

"forcedtimeout":true,

"forcedtimeoutwarning":true,

"ntdomain":true,

"clientlessvpnmode":true,

"emailhome":true,

"clientlessmodeurlencoding":true,

"clientlesspersistentcookie":true,

"allowedlogingroups":true,

"securebrowse":true,

"storefronturl":true,

"sfgatewayauthtype":true,

"kcdaccount":true,

"rdpclientprofilename":true,

"windowspluginupgrade":true,

"macpluginupgrade":true,

"linuxpluginupgrade":true,

"iconwithreceiver":true,
```

```
"alwaysonprofilename":true,

"autoproxyurl":true,

"advancedclientlessvpnmode":true,

"pcoipprofilename":true,

"fqdnspoofedip":true,

"netmask":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnsessionaction **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/vpnsessionaction? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/vpnsessionaction? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of vpnsessionaction resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/vpnsessionaction? **view=summary**

Use this query-parameter to get the summary output of vpnsessionaction resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/vpnsessionaction? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vpnsessionaction resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vpnsessionaction": [ {

"name":<String_value>,

"useraccounting":<String_value>,

"httpport":<Integer[]_value>,

"winsip":<String_value>,

"dnsvservername":<String_value>,

"splitdns":<String_value>,

"sesstimeout":<Integer_value>,

"clientsecurity":<String_value>,

"clientsecuritygroup":<String_value>,

"clientsecuritymessage":<String_value>,

"clientsecuritylog":<String_value>,
```

```
"splittunnel":<String_value>,

"locallanaccess":<String_value>,

"rfc1918":<String_value>,

"spoofiip":<String_value>,

"killconnections":<String_value>,

"transparentinterception":<String_value>,

"windowsclienttype":<String_value>,

"defaultauthorizationaction":<String_value>,

"authorizationgroup":<String_value>,

"smartgroup":<String_value>,

"clientidletimeout":<Integer_value>,

"clientidletimeoutwarning":<Integer_value>,

"proxy":<String_value>,

"allprotocolproxy":<String_value>,

"httpproxy":<String_value>,

"ftpproxy":<String_value>,

"socksproxy":<String_value>,

"gopherproxy":<String_value>,

"sslproxy":<String_value>,

"proxyexception":<String_value>,

"proxylocalbypass":<String_value>,

"clientcleanupprompt":<String_value>,
```

```
"forcecleanup":<String[]_value>,

"clientoptions":<String_value>,

"clientconfiguration":<String[]_value>,

"sso":<String_value>,

"ssocredential":<String_value>,

"windowsautologon":<String_value>,

"usemip":<String_value>,

"useiip":<String_value>,

"clientdebug":<String_value>,

"loginscript":<String_value>,

"logoutscript":<String_value>,

"homepage":<String_value>,

"icaproxy":<String_value>,

"wihome":<String_value>,

"wihomeaddresstype":<String_value>,

"citrixreceiverhome":<String_value>,

"wiportalmode":<String_value>,

"clientchoices":<String_value>,

"epaclienttype":<String_value>,

"iipdnssuffix":<String_value>,

"forcedtimeout":<Integer_value>,

"forcedtimeoutwarning":<Integer_value>,
```

```
"ntdomain":<String_value>,

"clientlessvpnmode":<String_value>,

"clientlessmodeurlencoding":<String_value>,

"clientlesspersistentcookie":<String_value>,

"emailhome":<String_value>,

"allowedlogingroups":<String_value>,

"securebrowse":<String_value>,

"storefronturl":<String_value>,

"sfgatewayauthtype":<String_value>,

"kcdaccount":<String_value>,

"rdpclientprofilename":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"windowspluginupgrade":<String_value>,

"macpluginupgrade":<String_value>,

"linuxpluginupgrade":<String_value>,

"iconwithreceiver":<String_value>,

"alwaysonprofilename":<String_value>,

"autoproxyurl":<String_value>,

"advancedclientlessvpnmode":<String_value>,

"pcoipprofilename":<String_value>,

"fqdnspoofedip":<String_value>,
```

```
"netmask":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnsessionaction/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/vpnsessionaction/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/vpnsessionaction/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of vpnsessionaction resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnsessionaction": [ {

"name":<String_value>,

"useraccounting":<String_value>,

"httpport":<Integer[]_value>,

"winsip":<String_value>,

"dnsvservername":<String_value>,

"splitdns":<String_value>,

"sesstimeout":<Integer_value>,

"clientsecurity":<String_value>,

"clientsecuritygroup":<String_value>,

"clientsecuritymessage":<String_value>,

"clientsecuritylog":<String_value>,

"splittunnel":<String_value>,

"locallanaccess":<String_value>,

"rfc1918":<String_value>,

"spoofiip":<String_value>,

"killconnections":<String_value>,

"transparentinterception":<String_value>,

"windowsclienttype":<String_value>,

"defaultauthorizationaction":<String_value>,

"authorizationgroup":<String_value>,

"smartgroup":<String_value>,
```

```
"clientidletimeout":<Integer_value>,

"clientidletimeoutwarning":<Integer_value>,

"proxy":<String_value>,

"allprotocolproxy":<String_value>,

"httpproxy":<String_value>,

"ftpproxy":<String_value>,

"socksproxy":<String_value>,

"gopherproxy":<String_value>,

"sslproxy":<String_value>,

"proxyexception":<String_value>,

"proxylocalbypass":<String_value>,

"clientcleanupprompt":<String_value>,

"forcecleanup":<String[]_value>,

"clientoptions":<String_value>,

"clientconfiguration":<String[]_value>,

"sso":<String_value>,

"ssocredential":<String_value>,

"windowsautologon":<String_value>,

"usemip":<String_value>,

"useiip":<String_value>,

"clientdebug":<String_value>,

"loginscript":<String_value>,
```

```
"logoutscript":<String_value>,

"homepage":<String_value>,

"icaproxy":<String_value>,

"wihome":<String_value>,

"wihomeaddresstype":<String_value>,

"citrixreceiverhome":<String_value>,

"wiportalmode":<String_value>,

"clientchoices":<String_value>,

"epaclienttype":<String_value>,

"iipdnssuffix":<String_value>,

"forcedtimeout":<Integer_value>,

"forcedtimeoutwarning":<Integer_value>,

"ntdomain":<String_value>,

"clientlessvpnmode":<String_value>,

"clientlessmodeurlencoding":<String_value>,

"clientlesspersistentcookie":<String_value>,

"emailhome":<String_value>,

"allowedlogingroups":<String_value>,

"securebrowse":<String_value>,

"storefronturl":<String_value>,

"sfgatewayauthtype":<String_value>,

"kcdaccount":<String_value>,
```

```
"rdpclientprofilename":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"windowspluginupgrade":<String_value>,

"macpluginupgrade":<String_value>,

"linuxpluginupgrade":<String_value>,

"iconwithreceiver":<String_value>,

"alwaysonprofilename":<String_value>,

"autoproxyurl":<String_value>,

"advancedclientlessvpnmode":<String_value>,

"pcoipprofilename":<String_value>,

"fqdnspoofedip":<String_value>,

"netmask":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnsessionaction? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vpnsessionaction": [ { "__count": "#no"} ] }
```

vpnsessionpolicy

Configuration for VPN session policy resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the new session policy that is applied after the user logs on to Citrix Gateway. Minimum length = 1
rule	<String>	Read-write	Expression, or name of a named expression, specifying the traffic that matches the policy. The following requirements apply only to the Citrix ADC CLI: * If the expression includes one or more spaces,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			enclose the entire expression in double quotation marks. * If the expression itself includes double quotation marks, escape the quotations by using the \ character. * Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks.
action	<String>	Read-write	Action to be applied by the new session policy if the rule criteria are met. Minimum length = 1
builtin	<String[]>	Read-only	Indicates that a variable is a built-in (SYSTEM INTERNAL) type. Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
feature	<String>	Read-only	The feature to be checked while applying this config.
expressiontype	<String>	Read-only	Type of policy (Classic/Advanced) . Possible values = Classic Policy, Advanced Policy
hits	<Integer>	Read-only	Number of hits.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnsessionpolicy **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"vpnsessionpolicy":{

<b>"name":<String_value>,

</b><b>"rule":<String_value>,

</b><b>"action":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnsessionpolicy/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnsessionpolicy **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"vpnsessionpolicy":{

<b>"name":<String_value>,

</b>"rule":<String_value>,

"action":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnsessionpolicy? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"vpnsessionpolicy":{

<b>"name":<String_value>,

</b>"rule":true,

"action":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnsessionpolicy **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/vpnsessionpolicy? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/vpnsessionpolicy? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of vpnsessionpolicy resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/vpnsessionpolicy? **view=summary**

Use this query-parameter to get the summary output of vpnsessionpolicy resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/vpnsessionpolicy? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vpnsessionpolicy resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vpnsessionpolicy": [ {

"name":<String_value>,

"rule":<String_value>,

"action":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"expressiontype":<String_value>,

"hits":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnsessionpolicy/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/vpnsessionpolicy/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/vpnsessionpolicy/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of vpnsessionpolicy resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnsessionpolicy": [ {

"name":<String_value>,

"rule":<String_value>,

"action":<String_value>,
```

```
"builtin":<String[]_value>,

"feature":<String_value>,

"expressiontype":<String_value>,

"hits":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnsessionpolicy? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vpnsessionpolicy": [ { "__count": "#no"} ] }
```

vpnsessionpolicy_aaagroup_binding

Binding object showing the aaagroup that can be bound to vpnsessionpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
boundto	<String>	Read-write	The entity name to which policy is bound.
name	<String>	Read-write	Name of the session policy to display. Minimum length = 1
priority	<Integer>	Read-only	.
activepolicy	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnsessionpolicy_aaagroup_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ vpnsessionpolicy_aaagroup_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of vpnsessionpolicy_aaagroup_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/vpnsessionpolicy_aaagroup_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vpnsessionpolicy_aaagroup_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnsessionpolicy_aaagroup_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"priority":<Integer_value>,

"activepolicy":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnsessionpolicy_aaagroup_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/vpnsessionpolicy_aaagroup_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnsessionpolicy_aaagroup_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"priority":<Integer_value>,

"activepolicy":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnsessionpolicy_aaagroup_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"vpnsessionpolicy_aaagroup_binding": [ { "__count": "#no"} ] }
```

vpnsessionpolicy_aaauser_binding

Binding object showing the aaauser that can be bound to vpnsessionpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the session policy to display. Minimum length = 1
boundto	<String>	Read-write	The entity name to which policy is bound.
activepolicy	<Integer>	Read-only	.
priority	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnsessionpolicy_aaauser_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ vpnsessionpolicy_aaauser_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of vpnsessionpolicy_aaauser_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/vpnsessionpolicy_aaauser_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vpnsessionpolicy_aaauser_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnsessionpolicy_aaauser_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"activepolicy":<Integer_value>,

"priority":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnsessionpolicy_aaauser_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/vpnsessionpolicy_aaauser_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnsessionpolicy_aaauser_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"activepolicy":<Integer_value>,

"priority":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnsessionpolicy_aaauser_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"vpnsessionpolicy_aaauser_binding": [ { "__count": "#no"} ] }
```

vpnsessionpolicy_binding

Binding object which returns the resources bound to vpnsessionpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the session policy to display. Minimum length = 1
vpnsessionpolicy_vpnvserver_binding	<vpnsessionpolicy_vpnvserver_binding[]>	Read-only	vpnvserver that can be bound to vpnsessionpolicy.
vpnsessionpolicy_vpnglobal_binding	<vpnsessionpolicy_vpnglobal_binding[]>	Read-only	vpnglobal that can be bound to vpnsessionpolicy.
vpnsessionpolicy_aaagroup_binding	<vpnsessionpolicy_aaagroup_binding[]>	Read-only	aaagroup that can be bound to vpnsessionpolicy.
vpnsessionpolicy_aaauser_binding	<vpnsessionpolicy_aaauser_binding[]>	Read-only	aaauser that can be bound to vpnsessionpolicy.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of

creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnsessionpolicy_binding/ name_value<String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vpnsessionpolicy_binding": [ {

"name":<String_value>,

"vpnsessionpolicy_aaagroup_binding":<vpnsessionpolicy_aaagroup_binding[]_v
alue>,

"vpnsessionpolicy_vpnglobal_binding":<vpnsessionpolicy_vpnglobal_binding[]
```

```
_value>,

"vpnsessionpolicy_aaauser_binding":<vpnsessionpolicy_aaauser_binding[]_val
ue>,

"vpnsessionpolicy_vpnvserver_binding":<vpnsessionpolicy_vpnvserver_binding
[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnsessionpolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/vpnsessionpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vpnsessionpolicy_binding": [ {

"name":<String_value>,

"vpnsessionpolicy_aaagroup_binding":<vpnsessionpolicy_aaagroup_binding[]_v
alue>,
```

```
"vpnsessionpolicy_vpnglobal_binding":<vpnsessionpolicy_vpnglobal_binding[]
_value>,

"vpnsessionpolicy_aaauser_binding":<vpnsessionpolicy_aaauser_binding[]_val
ue>,

"vpnsessionpolicy_vpnvserver_binding":<vpnsessionpolicy_vpnvserver_binding
[]_value>

}]}
```

vpnsessionpolicy_vpnglobal_binding

Binding object showing the vpnglobal that can be bound to vpnsessionpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the session policy to display. Minimum length = 1
boundto	<String>	Read-write	The entity name to which policy is bound.
priority	<Integer>	Read-only	.
activepolicy	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnsessionpolicy_vpnglobal_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ vpnsessionpolicy_vpnglobal_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of vpnsessionpolicy_vpnglobal_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/vpnsessionpolicy_vpnglobal_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vpnsessionpolicy_vpnglobal_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnsessionpolicy_vpnglobal_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"priority":<Integer_value>,

"activepolicy":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnsessionpolicy_vpnglobal_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/vpnsessionpolicy_vpnglobal_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnsessionpolicy_vpnglobal_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"priority":<Integer_value>,

"activepolicy":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnsessionpolicy_vpnglobal_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"vpnsessionpolicy_vpnglobal_binding": [ { "__count": "#no"} ] }
```

vpnsessionpolicy_vpnvserver_binding

Binding object showing the vpnvserver that can be bound to vpnsessionpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the session policy to display. Minimum length = 1
boundto	<String>	Read-write	The entity name to which policy is bound.
priority	<Integer>	Read-only	.
activepolicy	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnsessionpolicy_vpnvserver_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ vpnsessionpolicy_vpnvserver_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of vpnsessionpolicy_vpnvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/vpnsessionpolicy_vpnvserver_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vpnsessionpolicy_vpnvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnsessionpolicy_vpnvserver_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"priority":<Integer_value>,

"activepolicy":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnsessionpolicy_vpnvserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/vpnsessionpolicy_vpnvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnsessionpolicy_vpnvserver_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"priority":<Integer_value>,

"activepolicy":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnsessionpolicy_vpnvserver_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"vpnsessionpolicy_vpnvserver_binding": [ { "__count": "#no"} ] }
```

vpnsfconfig

Configuration for Create a StoreFront configuration file resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
vserver	<String[]>	Read-write	Name of Gateway virtual server.
filename	<String>	Read-only	Path where file was created.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.
- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of

creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnsfconfig

Query-parameters:

args

http:// <netscaler-ip-address> /nitro/v1/config/vpnsfconfig? **args=vserver: <String_value>**

Use this query-parameter to get vpnsfconfig resources based on additional properties.

attrs

http:// <netscaler-ip-address> /nitro/v1/config/vpnsfconfig? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter

http:// <netscaler-ip-address> /nitro/v1/config/vpnsfconfig? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of vpnsfconfig resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view

http:// <netscaler-ip-address> /nitro/v1/config/vpnsfconfig? **view=summary**

Use this query-parameter to get the summary output of vpnsfconfig resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination

http:// <netscaler-ip-address> /nitro/v1/config/vpnsfconfig? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vpnsfconfig resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vpnsfconfig": [ {

vserver:<String[]_value>"filename":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnsfconfig? **count=yes**

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response:

HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vpnsfconfig": [ { "__count": "#no"} ] }
```

vpnstoreinfo

Configuration for Store information for a URL resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
url	<String>	Read-write	StoreFront URL to be scanned.
storeserverstatus	<String>	Read-only	Availability of the server for TCP connections.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = UP, DOWN
storeserverissf	<String>	Read-only	Indicates if the server being scanned is running StoreFront. Possible values = YES, NO
storeapisupport	<String>	Read-only	Indicates StoreFront API support status. Possible values = YES, NO
storelist	<String>	Read-only	List of available stores return by StoreFront API.
storestatus	<String>	Read-only	Availability of the specified StoreFront store. Possible values = UP, DOWN
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnstoreinfo **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/vpnstoreinfo? **args= url:<String_value>,**

Use this query-parameter to get vpnstoreinfo resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/config/vpnstoreinfo? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/vpnstoreinfo? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of vpnstoreinfo resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/vpnstoreinfo? **view=summary**

Use this query-parameter to get the summary output of vpnstoreinfo resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/vpnstoreinfo? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vpnstoreinfo resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vpnstoreinfo": [ {

<b>url:<String_value>,</b>"storeserverstatus":<String_value>,

"storeserverissf":<String_value>,

"storeapisupport":<String_value>,

"storelist":<String_value>,

"storestatus":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnstoreinfo? **args= url:<String_value>, ;count=yes**
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vpnstoreinfo": [ { "__count": "#no"} ] }
```

vpntrafficaction

Configuration for VPN traffic action resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the traffic action. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after a traffic action is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my action" or 'my action'). Minimum length = 1
qual	<String>	Read-write	Protocol, either HTTP or TCP, to be used with the action. Possible values = http, tcp
apptimeout	<Integer>	Read-write	Maximum amount of time, in minutes, a user can stay logged on to the web application. Minimum value = 1 Maximum value = 715827

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
sso	<String>	Read-write	Provide single sign-on to the web application. NOTE : Authentication mechanisms like Basic-authentication require the user credentials to be sent in plaintext which is not secure if the server is running on HTTP (instead of HTTPS). Possible values = ON, OFF
hdx	<String>	Read-write	Provide hdx proxy to the ICA traffic. Possible values = ON, OFF
formssoaction	<String>	Read-write	Name of the form-based single sign-on profile. Form-based single sign-on allows users to log on one time to all protected applications in your network, instead of requiring them to log on separately to access each one.
fta	<String>	Read-write	Specify file type association, which is a list of file

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			extensions that users are allowed to open. Possible values = ON, OFF
wanscaler	<String>	Read-write	Use the Repeater Plug-in to optimize network traffic. Possible values = ON, OFF
kcdaccount	<String>	Read-write	Kerberos constrained delegation account name. Default value: "Default" Minimum length = 1 Maximum length = 32
samlssoprofile	<String>	Read-write	Profile to be used for doing SAML SSO to remote relying party. Minimum length = 1
proxy	<String>	Read-write	IP address and Port of the proxy server to be used for HTTP access for this request. Minimum length = 1
userexpression	<String>	Read-write	expression that will be evaluated to obtain username for SingleSignOn.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum length = 256
passwdexpression	<String>	Read-write	expression that will be evaluated to obtain password for SingleSignOn. Maximum length = 256
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of

creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpntrafficaction **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"vpntrafficaction":{

<b>"name":<String_value>,

</b><b>"qual":<String_value>,

</b>"apptimeout":<Integer_value>,

"sso":<String_value>,

"hdx":<String_value>,

"formssoaction":<String_value>,

"fta":<String_value>,

"wanscaler":<String_value>,
```

```
"kcdaccount":<String_value>,

"samlssoprofile":<String_value>,

"proxy":<String_value>,

"userexpression":<String_value>,

"passwdexpression":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpntrafficaction/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpntrafficaction **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"vpntrafficaction":{

<b>"name":<String_value>,

</b>"apptimeout":<Integer_value>,

"sso":<String_value>,

"hdx":<String_value>,

"formssoaction":<String_value>,

"fta":<String_value>,

"wanscaler":<String_value>,

"kcdaccount":<String_value>,

"samlssoprofile":<String_value>,

"proxy":<String_value>,

"userexpression":<String_value>,

"passwdexpression":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpntrafficaction? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"vpntrafficaction":{

<b>"name":<String_value>,

</b>"wanscaler":true,

"kcdaccount":true,

"proxy":true,

"userexpression":true,

"passwdexpression":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpntrafficaction **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/vpntrafficaction? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/vpntrafficaction? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of vpntrafficaction resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/vpntrafficaction? **view=summary**

Use this query-parameter to get the summary output of vpntrafficaction resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/vpntrafficaction?**pagesize=#no;pageno=#no**

Use this query-parameter to get the vpntrafficaction resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vpntrafficaction": [ {

"name":<String_value>,

"qual":<String_value>,

"apptimeout":<Integer_value>,

"sso":<String_value>,

"formssoaction":<String_value>,

"hdx":<String_value>,

"fta":<String_value>,

"wanscaler":<String_value>,

"kcdaccount":<String_value>,
```

```
"samlssoprofile":<String_value>,

"proxy":<String_value>,

"userexpression":<String_value>,

"passwdexpression":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpntrafficaction/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/vpntrafficaction/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/vpntrafficaction/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of vpntrafficaction resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpntrafficaction": [ {

"name":<String_value>,

"qual":<String_value>,

"apptimeout":<Integer_value>,

"sso":<String_value>,

"formssoaction":<String_value>,

"hdx":<String_value>,

"fta":<String_value>,

"wanscaler":<String_value>,

"kcdaccount":<String_value>,

"samlssoprofile":<String_value>,

"proxy":<String_value>,

"userexpression":<String_value>,

"passwdexpression":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpntrafficaction? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vpntrafficaction": [ { "__count": "#no"} ] }
```

vpntrafficpolicy

Configuration for VPN traffic policy resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the traffic policy. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the policy is created.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my policy" or 'my policy'). Minimum length = 1
rule	<String>	Read-write	Expression, or name of a named expression, against which traffic is evaluated. The following requirements apply only to the Citrix ADC CLI: * If the expression includes one or more spaces, enclose the entire expression in double quotation marks. * If the expression itself includes double quotation marks, escape the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			quotations by using the \ character. * Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks.
action	<String>	Read-write	Action to apply to traffic that matches the policy. Minimum length = 1
expressiontype	<String>	Read-only	Type of policy (Classic/Advanced). Possible values = Classic Policy, Advanced Policy
hits	<Integer>	Read-only	Number of hits.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)

- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpntrafficpolicy **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"vpntrafficpolicy":{

<b>"name":<String_value>,

</b><b>"rule":<String_value>,

</b><b>"action":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpntrafficpolicy/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpntrafficpolicy **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"vpntrafficpolicy":{

<b>"name":<String_value>,
```

```
</b>"rule":<String_value>,

"action":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpntrafficpolicy? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"vpntrafficpolicy":{

<b>"name":<String_value>,

</b>"rule":true,

"action":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpntrafficpolicy **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/vpntrafficpolicy? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/vpntrafficpolicy? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of vpntrafficpolicy resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/vpntrafficpolicy? **view=summary**

Use this query-parameter to get the summary output of vpntrafficpolicy resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/vpntrafficpolicy? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vpntrafficpolicy resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vpntrafficpolicy": [ {

"name":<String_value>,

"rule":<String_value>,

"action":<String_value>,

"expressiontype":<String_value>,

"hits":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpntrafficpolicy/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/vpntrafficpolicy/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/vpntrafficpolicy/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of vpntrafficpolicy resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpntrafficpolicy": [ {

"name":<String_value>,

"rule":<String_value>,

"action":<String_value>,

"expressiontype":<String_value>,

"hits":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpntrafficpolicy? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vpntrafficpolicy": [ { "__count": "#no"} ] }
```

vpntrafficpolicy_aaagroup_binding

Binding object showing the aaagroup that can be bound to vpntrafficpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
boundto	<String>	Read-write	The entity name to which policy is bound.
name	<String>	Read-write	Name of the traffic policy for which to display detailed information. Minimum length = 1
activepolicy	<Integer>	Read-only	.
priority	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpntrafficpolicy_aaagroup_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ vpntrafficpolicy_aaagroup_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of vpntrafficpolicy_aaagroup_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/vpntrafficpolicy_aaagroup_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vpntrafficpolicy_aaagroup_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpntrafficpolicy_aaagroup_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"activepolicy":<Integer_value>,

"priority":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpntrafficpolicy_aaagroup_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/vpntrafficpolicy_aaagroup_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpntrafficpolicy_aaagroup_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"activepolicy":<Integer_value>,

"priority":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpntrafficpolicy_aaagroup_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"vpntrafficpolicy_aaagroup_binding": [ { "__count": "#no"} ] }
```

vpntrafficpolicy_aaauser_binding

Binding object showing the aaauser that can be bound to vpntrafficpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
boundto	<String>	Read-write	The entity name to which policy is bound.
name	<String>	Read-write	Name of the traffic policy for which to display detailed information. Minimum length = 1
activepolicy	<Integer>	Read-only	.
priority	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpntrafficpolicy_aaauser_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ vpntrafficpolicy_aaauser_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of vpntrafficpolicy_aaauser_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/vpntrafficpolicy_aaauser_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vpntrafficpolicy_aaauser_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpntrafficpolicy_aaauser_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"activepolicy":<Integer_value>,

"priority":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpntrafficpolicy_aaauser_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/vpntrafficpolicy_aaauser_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpntrafficpolicy_aaauser_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"activepolicy":<Integer_value>,

"priority":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpntrafficpolicy_aaauser_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"vpntrafficpolicy_aaauser_binding": [ { "__count": "#no"} ] }
```

vpntrafficpolicy_binding

Binding object which returns the resources bound to vpntrafficpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the traffic policy for which to display detailed information. Minimum length = 1
vpntrafficpolicy_vpnvserver_binding	<vpntrafficpolicy_vpnvserver_binding[]>	Read-only	vpnvserver that can be bound to vpntrafficpolicy.
vpntrafficpolicy_aaagroup_binding	<vpntrafficpolicy_aaagroup_binding[]>	Read-only	aaagroup that can be bound to vpntrafficpolicy.
vpntrafficpolicy_vpnglobal_binding	<vpntrafficpolicy_vpnglobal_binding[]>	Read-only	vpnglobal that can be bound to vpntrafficpolicy.
vpntrafficpolicy_aaauser_binding	<vpntrafficpolicy_aaauser_binding[]>	Read-only	aaauser that can be bound to vpntrafficpolicy.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpntrafficpolicy_binding/ name_value<String>
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vpntrafficpolicy_binding": [ {

"name":<String_value>,

"vpntrafficpolicy_vpnglobal_binding":<vpntrafficpolicy_vpnglobal_binding[]
_value>,

"vpntrafficpolicy_aaauser_binding":<vpntrafficpolicy_aaauser_binding[]_val
ue>,

"vpntrafficpolicy_vpnvserver_binding":<vpntrafficpolicy_vpnvserver_binding
[]_value>,

"vpntrafficpolicy_aaagroup_binding":<vpntrafficpolicy_aaagroup_binding[]_v
alue>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpntrafficpolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/vpntrafficpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vpntrafficpolicy_binding": [ {

"name":<String_value>,

"vpntrafficpolicy_vpnglobal_binding":<vpntrafficpolicy_vpnglobal_binding[]
_value>,

"vpntrafficpolicy_aaauser_binding":<vpntrafficpolicy_aaauser_binding[]_val
ue>,

"vpntrafficpolicy_vpnvserver_binding":<vpntrafficpolicy_vpnvserver_binding
[]_value>,

"vpntrafficpolicy_aaagroup_binding":<vpntrafficpolicy_aaagroup_binding[]_v
alue>

}]}
```

vpntrafficpolicy_vpnglobal_binding

Binding object showing the vpnglobal that can be bound to vpntrafficpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
boundto	<String>	Read-write	The entity name to which policy is bound.
name	<String>	Read-write	Name of the traffic policy for which to display detailed information. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
activepolicy	<Integer>	Read-only	.
priority	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpntrafficpolicy_vpnglobal_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ vpntrafficpolicy_vpnglobal_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of vpntrafficpolicy_vpnglobal_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/vpntrafficpolicy_vpnglobal_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vpntrafficpolicy_vpnglobal_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpntrafficpolicy_vpnglobal_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"activepolicy":<Integer_value>,

"priority":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpntrafficpolicy_vpnglobal_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/vpntrafficpolicy_vpnglobal_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpntrafficpolicy_vpnglobal_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"activepolicy":<Integer_value>,

"priority":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpntrafficpolicy_vpnglobal_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"vpntrafficpolicy_vpnglobal_binding": [ { "__count": "#no"} ] }
```

vpntrafficpolicy_vpnvserver_binding

Binding object showing the vpnvserver that can be bound to vpntrafficpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
boundto	<String>	Read-write	The entity name to which policy is bound.
name	<String>	Read-write	Name of the traffic policy for which to display detailed information. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
priority	<Integer>	Read-only	.
activepolicy	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpntrafficpolicy_vpnvserver_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ vpntrafficpolicy_vpnvserver_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of vpntrafficpolicy_vpnvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/vpntrafficpolicy_vpnvserver_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vpntrafficpolicy_vpnvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpntrafficpolicy_vpnvserver_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"priority":<Integer_value>,

"activepolicy":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpntrafficpolicy_vpnvserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/vpntrafficpolicy_vpnvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpntrafficpolicy_vpnvserver_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"priority":<Integer_value>,

"activepolicy":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpntrafficpolicy_vpnvserver_binding/name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"vpntrafficpolicy_vpnvserver_binding": [ { "__count": "#no"} ] }
```

vpnurl

Configuration for VPN URL resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
urlname	<String>	Read-write	Name of the bookmark link. Minimum length = 1
linkname	<String>	Read-write	Description of the bookmark link. The description appears in the Access Interface. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
actualurl	<String>	Read-write	Web address for the bookmark link. Minimum length = 1
vservername	<String>	Read-write	Name of the associated LB/CS vserver.
clientlessaccess	<String>	Read-write	If clientless access to the resource hosting the link is allowed, also use clientless access for the bookmarked web address in the Secure Client Access based session. Allows single sign-on and other HTTP processing on Citrix Gateway for HTTPS resources. Default value: OFF Possible values = ON, OFF
comment	<String>	Read-write	Any comments associated with the bookmark link.
iconurl	<String>	Read-write	URL to fetch icon file for displaying this resource.
ssotype	<String>	Read-write	Single sign on type for unified gateway. Possible values = unifiedgateway, selfauth, samlauth

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
applicationtype	<String>	Read-write	The type of application this VPN URL represents. Possible values are CVPN/SaaS/VPN. Possible values = CVPN, VPN, SaaS
samlssoprofile	<String>	Read-write	Profile to be used for doing SAML SSO.
appjson	<String>	Read-write	To store the template details in the json format.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnurl **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"vpnurl":{

<b>"urlname":<String_value>,

</b><b>"linkname":<String_value>,

</b><b>"actualurl":<String_value>,

</b>"vservername":<String_value>,

"clientlessaccess":<String_value>,

"comment":<String_value>,
```

```
"iconurl":<String_value>,

"ssotype":<String_value>,

"applicationtype":<String_value>,

"samlssoprofile":<String_value>,

"appjson":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnurl/ urlname_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnurl **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"vpnurl":{

<b>"urlname":<String_value>,

</b>"linkname":<String_value>,

"actualurl":<String_value>,

"vservername":<String_value>,

"clientlessaccess":<String_value>,

"comment":<String_value>,

"iconurl":<String_value>,

"ssotype":<String_value>,

"applicationtype":<String_value>,

"samlssoprofile":<String_value>,

"appjson":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnurl? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"vpnurl":{

<b>"urlname":<String_value>,

</b>"vservername":true,

"clientlessaccess":true,

"comment":true,

"iconurl":true,

"ssotype":true,

"applicationtype":true,

"samlssoprofile":true,

"appjson":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnurl **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/vpnurl? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/vpnurl? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of vpnurl resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/vpnurl? **view=summary**

Use this query-parameter to get the summary output of vpnurl resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/vpnurl? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vpnurl resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vpnurl": [ {

"urlname":<String_value>,

"linkname":<String_value>,

"vservername":<String_value>,

"actualurl":<String_value>,

"clientlessaccess":<String_value>,

"comment":<String_value>,

"iconurl":<String_value>,

"ssotype":<String_value>,

"applicationtype":<String_value>,
```

```
"samlssoprofile":<String_value>,

"appjson":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnurl/ urlname_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/vpnurl/ urlname_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/vpnurl/ urlname_value<String> ? **view=summary**

Use this query-parameter to get the summary output of vpnurl resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnurl": [ {

"urlname":<String_value>,

"linkname":<String_value>,

"vservername":<String_value>,

"actualurl":<String_value>,

"clientlessaccess":<String_value>,

"comment":<String_value>,

"iconurl":<String_value>,

"ssotype":<String_value>,

"applicationtype":<String_value>,

"samlssoprofile":<String_value>,

"appjson":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnurl? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vpnurl": [ { "__count": "#no"} ] }
```

vpnurlaction

Configuration for VPN url action resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the bookmark link. Minimum length = 1
linkname	<String>	Read-write	Description of the bookmark link. The description appears in the Access Interface. Minimum length = 1
actualurl	<String>	Read-write	Web address for the bookmark link. Minimum length = 1
vservername	<String>	Read-write	Name of the associated vserver to handle selfAuth SSO.
clientlessaccess	<String>	Read-write	If clientless access to the resource hosting the link is allowed, also use clientless access for the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			bookmarked web address in the Secure Client Access based session. Allows single sign-on and other HTTP processing on NetScaler Gateway for HTTPS resources. Default value: OFF Possible values = ON, OFF
comment	<String>	Read-write	Any comments associated with the bookmark link.
iconurl	<String>	Read-write	URL to fetch icon file for displaying this resource.
ssotype	<String>	Read-write	Single sign on type for unified gateway. Possible values = unifiedgateway, selfauth, samlauth
applicationtype	<String>	Read-write	The type of application this VPN URL represents. Possible values are CVPN/SaaS/VPN. Possible values = CVPN, VPN, SaaS
samlssoprofile	<String>	Read-write	Profile to be used for doing SAML SSO.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
newname	<String>	Read-write	New name for the vpn urlAction. Must begin with a letter, number, or the underscore character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space ( ), at (@), equals (=), colon (:), and underscore characters. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my vpnurl action" or 'my vpnurl action'). Minimum length = 1
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT
- RENAME

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnurlaction **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"vpnurlaction":{

<b>"name":<String_value>,

</b><b>"linkname":<String_value>,

</b><b>"actualurl":<String_value>,

</b>"vservername":<String_value>,

"clientlessaccess":<String_value>,

"comment":<String_value>,

"iconurl":<String_value>,

"ssotype":<String_value>,

"applicationtype":<String_value>,

"samlssoprofile":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnurlaction/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnurlaction **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"vpnurlaction":{

<b>"name":<String_value>,

</b>"linkname":<String_value>,

"actualurl":<String_value>,

"vservername":<String_value>,

"clientlessaccess":<String_value>,

"comment":<String_value>,

"iconurl":<String_value>,

"ssotype":<String_value>,

"applicationtype":<String_value>,
```

```
"samlssoprofile":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnurlaction? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"vpnurlaction":{

<b>"name":<String_value>,

</b>"vservername":true,

"clientlessaccess":true,

"comment":true,

"iconurl":true,

"ssotype":true,

"applicationtype":true,

"samlssoprofile":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

RENAME

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnurlaction? **action=rename HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"vpnurlaction":{

<b>"name":<String_value>,

</b><b>"newname":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnurlaction **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/vpnurlaction? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/vpnurlaction? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of vpnurlaction resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/vpnurlaction? **view=summary**

Use this query-parameter to get the summary output of vpnurlaction resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/vpnurlaction? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vpnurlaction resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vpnurlaction": [ {

"name":<String_value>,

"linkname":<String_value>,

"vservername":<String_value>,

"actualurl":<String_value>,

"clientlessaccess":<String_value>,
```

```
"comment":<String_value>,

"iconurl":<String_value>,

"ssotype":<String_value>,

"applicationtype":<String_value>,

"samlssoprofile":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnurlaction/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/vpnurlaction/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/vpnurlaction/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of vpnurlaction resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnurlaction": [ {

"name":<String_value>,

"linkname":<String_value>,

"vservername":<String_value>,

"actualurl":<String_value>,

"clientlessaccess":<String_value>,

"comment":<String_value>,

"iconurl":<String_value>,

"ssotype":<String_value>,

"applicationtype":<String_value>,

"samlssoprofile":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnurlaction? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vpnurlaction": [ { "__count": "#no"} ] }
```

vpnurlpolicy

Configuration for VPN url policy resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the new urlPolicy. Minimum length = 1
rule	<String>	Read-write	Expression, or name of a named expression, specifying the traffic that matches the policy. The following requirements apply only to the NetScaler CLI: * If the expression includes one or more spaces, enclose the entire expression in

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			double quotation marks. * If the expression itself includes double quotation marks, escape the quotations by using the \ character. * Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape the double quotation marks.
action	<String>	Read-write	Action to be applied by the new urlPolicy if the rule criteria are met. Minimum length = 1
comment	<String>	Read-write	Any comments to preserve information about this policy.
logaction	<String>	Read-write	Name of messagelog action to use when a request matches this policy.
newname	<String>	Read-write	New name for the vpn urlPolicy. Must begin with a letter, number, or the underscore

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			character (_), and must contain only letters, numbers, and the hyphen (-), period (.) hash (#), space ( ), at (@), equals (=), colon (:), and underscore characters. The following requirement applies only to the NetScaler CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my vpnurl policy" or 'my vpnurl policy'). Minimum length = 1
builtin	<String[]>	Read-only	Indicates that a variable is a built-in (SYSTEM INTERNAL) type. Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
undefhits	<Integer>	Read-only	The number of times the policy evaluation resulted in undefined processing.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT
- RENAME

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.
- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnurlpolicy **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"vpnurlpolicy":{

<b>"name":<String_value>,

</b><b>"rule":<String_value>,

</b><b>"action":<String_value>,

</b>"comment":<String_value>,

"logaction":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnurlpolicy/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnurlpolicy **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"vpnurlpolicy":{

<b>"name":<String_value>,

</b>"rule":<String_value>,

"action":<String_value>,

"comment":<String_value>,

"logaction":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnurlpolicy? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"vpnurlpolicy":{

<b>"name":<String_value>,

</b>"comment":true,

"logaction":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

RENAME

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnurlpolicy? **action=rename HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"vpnurlpolicy":{

<b>"name":<String_value>,
```

```
</b><b>"newname":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnurlpolicy **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/vpnurlpolicy? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/vpnurlpolicy? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of vpnurlpolicy resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/vpnurlpolicy? **view=summary**

Use this query-parameter to get the summary output of vpnurlpolicy resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/vpnurlpolicy? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vpnurlpolicy resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vpnurlpolicy": [ {

"name":<String_value>,

"rule":<String_value>,

"action":<String_value>,

"comment":<String_value>,

"logaction":<String_value>,

"builtin":<String[]_value>,

"undefhits":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnurlpolicy/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/vpnurlpolicy/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/vpnurlpolicy/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of vpnurlpolicy resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnurlpolicy": [ {

"name":<String_value>,

"rule":<String_value>,

"action":<String_value>,

"comment":<String_value>,

"logaction":<String_value>,

"builtin":<String[]_value>,

"undefhits":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnurlpolicy? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vpnurlpolicy": [ { "__count": "#no"} ] }
```

vpnurlpolicy_aaagroup_binding

Binding object showing the aaagroup that can be bound to vpnurlpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the new urlPolicy. Minimum length = 1
boundto	<String>	Read-write	The entity name to which policy is bound.
priority	<Integer>	Read-only	.
activepolicy	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnurlpolicy_aaagroup_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ vpnurlpolicy_aaagroup_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of vpnurlpolicy_aaagroup_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/vpnurlpolicy_aaagroup_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vpnurlpolicy_aaagroup_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnurlpolicy_aaagroup_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"priority":<Integer_value>,

"activepolicy":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnurlpolicy_aaagroup_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/vpnurlpolicy_aaagroup_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnurlpolicy_aaagroup_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"priority":<Integer_value>,

"activepolicy":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnurlpolicy_aaagroup_binding/name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"vpnurlpolicy_aaagroup_binding": [ { "__count": "#no"} ] }
```

vpnurlpolicy_aaauser_binding

Binding object showing the aaauser that can be bound to vpnurlpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the new urlPolicy. Minimum length = 1
boundto	<String>	Read-write	The entity name to which policy is bound.
priority	<Integer>	Read-only	.
activepolicy	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET

- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnurlpolicy_aaauser_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ vpnurlpolicy_aaauser_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of vpnurlpolicy_aaauser_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/vpnurlpolicy_aaauser_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vpnurlpolicy_aaauser_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnurlpolicy_aaauser_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"priority":<Integer_value>,

"activepolicy":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnurlpolicy_aaauser_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/vpnurlpolicy_aaauser_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnurlpolicy_aaauser_binding": [ {

"name":<String_value>,

"boundto":<String_value>,

"priority":<Integer_value>,

"activepolicy":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnurlpolicy_aaauser_binding/name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"vpnurlpolicy_aaauser_binding": [ { "__count": "#no"} ] }
```

vpnurlpolicy_binding

Binding object which returns the resources bound to vpnurlpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the new urlPolicy. Minimum length = 1
vpnurlpolicy_aaauser_binding	<vpnurlpolicy_aaauser_binding[]>	Read-only	aaauser that can be bound to vpnurlpolicy.
vpnurlpolicy_vpnvserver_binding	<vpnurlpolicy_vpnvserver_binding[]>	Read-only	vpnvserver that can be bound to vpnurlpolicy.
vpnurlpolicy_vpnglobal_binding	<vpnurlpolicy_vpnglobal_binding[]>	Read-only	vpnglobal that can be bound to vpnurlpolicy.
vpnurlpolicy_aaagroup_binding	<vpnurlpolicy_aaagroup_binding[]>	Read-only	aaagroup that can be bound to vpnurlpolicy.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnurlpolicy_binding/ name_value<String>
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vpnurlpolicy_binding": [ {

"name":<String_value>,

"vpnurlpolicy_aaagroup_binding":<vpnurlpolicy_aaagroup_binding[]_value>,

"vpnurlpolicy_vpnvserver_binding":<vpnurlpolicy_vpnvserver_binding[]_value
>,

"vpnurlpolicy_aaauser_binding":<vpnurlpolicy_aaauser_binding[]_value>,

"vpnurlpolicy_vpnglobal_binding":<vpnurlpolicy_vpnglobal_binding[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnurlpolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/vpnurlpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vpnurlpolicy_binding": [ {

"name":<String_value>,

"vpnurlpolicy_aaagroup_binding":<vpnurlpolicy_aaagroup_binding[]_value>,

"vpnurlpolicy_vpnvserver_binding":<vpnurlpolicy_vpnvserver_binding[]_value
>,

"vpnurlpolicy_aaauser_binding":<vpnurlpolicy_aaauser_binding[]_value>,

"vpnurlpolicy_vpnglobal_binding":<vpnurlpolicy_vpnglobal_binding[]_value>

}]}
```

vpnurlpolicy_vpnglobal_binding

Binding object showing the vpnglobal that can be bound to vpnurlpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
boundto	<String>	Read-write	The entity name to which policy is bound.
name	<String>	Read-write	Name for the new urlPolicy. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
activepolicy	<Integer>	Read-only	.
priority	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnurlpolicy_vpnglobal_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ vpnurlpolicy_vpnglobal_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of vpnurlpolicy_vpnglobal_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/vpnurlpolicy_vpnglobal_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vpnurlpolicy_vpnglobal_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnurlpolicy_vpnglobal_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"activepolicy":<Integer_value>,

"priority":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnurlpolicy_vpnglobal_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/vpnurlpolicy_vpnglobal_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnurlpolicy_vpnglobal_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"activepolicy":<Integer_value>,

"priority":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnurlpolicy_vpnglobal_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"vpnurlpolicy_vpnglobal_binding": [ { "__count": "#no"} ] }
```

vpnurlpolicy_vpnvserver_binding

Binding object showing the vpnvserver that can be bound to vpnurlpolicy.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
boundto	<String>	Read-write	The entity name to which policy is bound.
name	<String>	Read-write	Name for the new urlPolicy. Minimum length = 1
priority	<Integer>	Read-only	.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
activepolicy	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnurlpolicy_vpnvserver_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ vpnurlpolicy_vpnvserver_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of vpnurlpolicy_vpnvserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/vpnurlpolicy_vpnvserver_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vpnurlpolicy_vpnvserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnurlpolicy_vpnvserver_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"priority":<Integer_value>,

"activepolicy":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnurlpolicy_vpnvserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/vpnurlpolicy_vpnvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnurlpolicy_vpnvserver_binding": [ {

"boundto":<String_value>,

"name":<String_value>,

"priority":<Integer_value>,

"activepolicy":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnurlpolicy_vpnvserver_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"vpnurlpolicy_vpnvserver_binding": [ { "__count": "#no"} ] }
```

vpnvserver

Configuration for VPN virtual server resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the Citrix Gateway virtual server. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			(#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Can be changed after the virtual server is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my server" or 'my server'). Minimum length = 1
servicetype	<String>	Read-write	Protocol used by the Citrix Gateway virtual server. Default value: SSL Possible values = SSL, DTLS, HTTP_QUIC
ipv46	<String>	Read-write	IPv4 or IPv6 address of the Citrix Gateway virtual server. Usually a public IP address. User devices send

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			connection requests to this IP address. Minimum length = 1
range	<Integer>	Read-write	Range of Citrix Gateway virtual server IP addresses. The consecutively numbered range of IP addresses begins with the address specified by the IP Address parameter. In the configuration utility, select Network VServer to enter a range. Default value: 1 Minimum value = 1
port	<Integer>	Read-write	TCP port on which the virtual server listens. Range 1 - 65535 * in CLI is represented as 65535 in NITRO API
ipset	<String>	Read-write	The list of IPv4/IPv6 addresses bound to ipset would form a part of listening service on the current vpn vserver. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
state	<String>	Read-write	State of the virtual server. If the virtual server is disabled, requests are not processed. Default value: ENABLED Possible values = ENABLED, DISABLED
authentication	<String>	Read-write	Require authentication for users connecting to Citrix Gateway. Default value: ON Possible values = ON, OFF
doublehop	<String>	Read-write	Use the Citrix Gateway appliance in a double-hop configuration. A double-hop deployment provides an extra layer of security for the internal network by using three firewalls to divide the DMZ into two stages. Such a deployment can have one appliance in the DMZ and one appliance in the secure network.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: DISABLED Possible values = ENABLED, DISABLED
maxaaausers	<Integer>	Read-write	Maximum number of concurrent user sessions allowed on this virtual server. The actual number of users allowed to log on to this virtual server depends on the total number of user licenses.
icaonly	<String>	Read-write	- When set to ON, it implies Basic mode where the user can log on using either Citrix Receiver or a browser and get access to the published apps configured at the XenApp/XenDEsktop environment pointed out by the WIHome parameter. Users are not allowed to connect using the Citrix Gateway Plug-in and end point scans cannot be configured. Number of users that can log in and access the apps are not limited

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			by the license in this mode. - When set to OFF, it implies Smart Access mode where the user can log on using either Citrix Receiver or a browser or a Citrix Gateway Plug-in. The admin can configure end point scans to be run on the client systems and then use the results to control access to the published apps. In this mode, the client can connect to the gateway in other client modes namely VPN and CVPN. Number of users that can log in and access the resources are limited by the CCU licenses in this mode. Default value: OFF Possible values = ON, OFF

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
icaproxysessionmigration	<String>	Read-write	This option determines if an existing ICA Proxy session is transferred when the user logs on from another device. Default value: OFF Possible values = ON, OFF
dtls	<String>	Read-write	This option starts/stops the turn service on the vserver. Default value: ON Possible values = ON, OFF
loginonce	<String>	Read-write	This option enables/disables seamless SSO for this Vserver. Default value: OFF Possible values = ON, OFF
advancedepa	<String>	Read-write	This option tells whether advanced EPA is enabled on this virtual server. Default value: OFF Possible values = ON, OFF
devicecert	<String>	Read-write	Indicates whether device certificate

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			check as a part of EPA is on or off. Default value: OFF Possible values = ON, OFF
certkeynames	<String>	Read-write	Name of the certificate key that was bound to the corresponding SSL virtual server as the Certificate Authority for the device certificate. Minimum length = 1 Maximum length = 127
downstateflush	<String>	Read-write	Close existing connections when the virtual server is marked DOWN, which means the server might have timed out. Disconnecting existing connections frees resources and in certain cases speeds recovery of overloaded load balancing setups. Enable this setting on servers in which the connections can safely be closed when they are marked DOWN. Do not enable DOWN

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			state flush on servers that must complete their transactions. Default value: ENABLED Possible values = ENABLED, DISABLED
listenpolicy	<String>	Read-write	String specifying the listen policy for the Citrix Gateway virtual server. Can be either a named expression or an expression. The Citrix Gateway virtual server processes only the traffic for which the expression evaluates to true. Default value: "none"
listenpriority	<Integer>	Read-write	Integer specifying the priority of the listen policy. A higher number specifies a lower priority. If a request matches the listen policies of more than one virtual server, the virtual server whose listen policy has the highest priority (the lowest priority

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			number) accepts the request. Default value: 101 Minimum value = 0 Maximum value = 100
tcpprofilename	<String>	Read-write	Name of the TCP profile to assign to this virtual server. Minimum length = 1 Maximum length = 127
httpprofilename	<String>	Read-write	Name of the HTTP profile to assign to this virtual server. Default value: "nshttp_default_strict_validation" Minimum length = 1 Maximum length = 127
comment	<String>	Read-write	Any comments associated with the virtual server.
appflowlog	<String>	Read-write	Log AppFlow records that contain standard NetFlow or IPFIX information, such as time stamps for the beginning and end of a flow, packet count, and byte count. Also

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			log records that contain application-level information, such as HTTP web addresses, HTTP request methods and response status codes, server response time, and latency. Default value: ENABLED Possible values = ENABLED, DISABLED
icmpvsrresponse	<String>	Read-write	Criterion for responding to PING requests sent to this virtual server. If this parameter is set to ACTIVE, respond only if the virtual server is available. With the PASSIVE setting, respond even if the virtual server is not available. Default value: PASSIVE Possible values = PASSIVE, ACTIVE
rhistate	<String>	Read-write	A host route is injected according to the setting on the virtual servers.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			* If set to PASSIVE on all the virtual servers that share the IP address, the appliance always injects the hostroute. * If set to ACTIVE on all the virtual servers that share the IP address, the appliance injects even if one virtual server is UP. * If set to ACTIVE on some virtual servers and PASSIVE on the others, the appliance injects even if one virtual server set to ACTIVE is UP. Default value: PASSIVE Possible values = PASSIVE, ACTIVE
netprofile	<String>	Read-write	The name of the network profile. Minimum length = 1 Maximum length = 127

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
cginfrahomepageredirect	<String>	Read-write	When client requests ShareFile resources and Citrix Gateway detects that the user is unauthenticated or the user session has expired, disabling this option takes the user to the originally requested ShareFile resource after authentication (instead of taking the user to the default VPN home page). Default value: ENABLED Possible values = ENABLED, DISABLED
secureprivateaccess	<String>	Read-write	Configure secure private access. Default value: DISABLED Possible values = ENABLED, DISABLED
accessrestrictedpageredirect	<String>	Read-write	By default, an access restricted page hosted on secure private access CDN is displayed when a restricted app is accessed. The setting can be

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			changed to NS to display the access restricted page hosted on the gateway or OFF to not display any access restricted page. Default value: CDN Possible values = CDN, NS, OFF
maxloginattempts	<Integer>	Read-write	Maximum number of logon attempts. Minimum value = 1 Maximum value = 255
failedlogintimeout	<Integer>	Read-write	Number of minutes an account will be locked if user exceeds maximum permissible attempts. Minimum value = 1
l2conn	<String>	Read-write	Use Layer 2 parameters (channel number, MAC address, and VLAN ID) in addition to the 4-tuple (<source IP>:<source port>::<destination IP>:<destination port>) that is used to identify a connection. Allows multiple TCP and non-TCP connections with the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			same 4-tuple to coexist on the Citrix ADC. Possible values = ON, OFF
deploymenttype	<String>	Read-write	. Default value: 5 Possible values = NONE, ICA_WEBINTERFACE, ICA_STOREFRONT, MOBILITY
rdpserverprofilename	<String>	Read-write	Name of the RDP server profile associated with the vserver. Minimum length = 1 Maximum length = 31
windowsepapluginupgrade	<String>	Read-write	Option to set plugin upgrade behaviour for Win. Possible values = Always, Essential, Never
linuxepapluginupgrade	<String>	Read-write	Option to set plugin upgrade behaviour for Linux. Possible values = Always, Essential, Never

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
macepapluginupgrade	<String>	Read-write	Option to set plugin upgrade behaviour for Mac. Possible values = Always, Essential, Never
logoutonsmartcardremoval	<String>	Read-write	Option to VPN plugin behavior when smartcard or its reader is removed. Default value: OFF Possible values = ON, OFF
userdomains	<String>	Read-write	List of user domains specified as comma seperated value.
authnprofile	<String>	Read-write	Authentication Profile entity on virtual server. This entity can be used to offload authentication to AAA vserver for multi-factor(nFactor) authentication.
vserverfqdn	<String>	Read-write	Fully qualified domain name for a VPN virtual server. This is used during StoreFront configuration generation.
gslbsitefqdn	<String>	Read-write	Fully qualified domain name of the SPA site. This is

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			used for Secure Private Access configuration.
pcoipvserverprofilename	<String>	Read-write	Name of the PCoIP vserver profile associated with the vserver. Minimum length = 1 Maximum length = 31
samesite	<String>	Read-write	SameSite attribute value for Cookies generated in VPN context. This attribute value will be appended only for the cookies which are specified in the builtin patset ns_cookies_samesite. Possible values = None, LAX, STRICT
quicprofilename	<String>	Read-write	Name of the QUIC profile to assign to this virtual server. Minimum length = 1 Maximum length = 127
deviceposture	<String>	Read-write	Enable device posture. Default value: DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ENABLED, DISABLED
wasmmodule	<String>	Read-write	Name of the WASM module to assign to this virtual server.
newname	<String>	Read-write	New name for the Citrix Gateway virtual server. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my server" or 'my server'). Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ip	<String>	Read-only	The Virtual IP address of the VPN virtual server.
value	<String>	Read-only	Indicates whether or not the certificate is bound or if SSL offload is disabled. Possible values = Certkey/ Certkeybundle/Vault not bound/Cert-store not usable, SSL feature disabled
type	<String>	Read-only	The type of virtual server; for example, CONTENT based or ADDRESS based. Possible values = CONTENT, ADDRESS
curstate	<String>	Read-only	The current state of the virtual server, as UP, DOWN, BUSY, and so on. Possible values = UP, DOWN, UNKNOWN, BUSY, OUT OF SERVICE, GOING OUT OF SERVICE, DOWN WHEN GOING OUT OF SERVICE, NS_EMPTY_STR,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Unknown, DISABLED
status	<Integer>	Read-only	Whether or not this virtual server responds to ARPs and whether or not round-robin selection is temporarily in effect.
cachetype	<String>	Read-only	Virtual server cache type. The options are: TRANSPARENT, REVERSE, and FORWARD. Possible values = TRANSPARENT, REVERSE, FORWARD
redirect	<String>	Read-only	The cache redirect policy. The valid redirect policies are: l. CACHE - Directs all requests to the cache. 2. POLICY - Applies cache redirection policy to determine whether the request should be directed to the cache or

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			origin. This is the default setting. 3. ORIGIN - Directs all requests to the origin server. Possible values = CACHE, POLICY, ORIGIN
precedence	<String>	Read-only	This argument is used only when configuring content switching on the specified virtual server. This is applicable only if both the URL and RULE-based policies have been configured on the same virtual server. It specifies the type of policy (URL or RULE) that takes precedence on the content switching virtual server. The default setting is RULE. l URL - In this case, the incoming request is matched against the URL-based policies

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			before the rule-based policies. l RULE - In this case, the incoming request is matched against the rule-based policies before the URL-based policies. For all URL-based policies, the precedence hierarchy is: 1. Domain and exact URL 2. Domain, prefix, and suffix 3. Domain and suffix 4. Domain and prefix 5. Domain only 6. Exact URL 7. Prefix and suffix 8. Suffix only 9. Prefix only 10. Default.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = RULE, URL
redirecturl	<String>	Read-only	The URL where traffic is redirected if the virtual server in system becomes unavailable. WARNING! Make sure that the domain you specify in the URL does not match the domain specified in the -d domainName argument of the ###add cs policy### command. If the same domain is specified in both arguments, the request will be continuously redirected to the same unavailable virtual server in the system. If so, the user may not get the requested content.
curaaausers	<Integer>	Read-only	The number of current users logged on to this virtual server.
curtotalusers	<Integer>	Read-only	The total number of current users connected through this virtual server.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
domain	<String>	Read-only	The domain name of the server for which a service needs to be added. If the IP address has been specified, the domain name does not need to be specified.
rule	<String>	Read-only	The name of the rule, or expression, if any, that policy for the VPN server is to use. Rules are combinations of expressions. Expressions are simple conditions, such as a test for equality, applied to operands, such as a URL string or an IP address. Expression syntax is described in the Installation and Configuration Guide. The default rule is true. Minimum length = 1
servicename	<String>	Read-only	The name of the service, if any, to which the virtual server policy is bound.
weight	<Integer>	Read-only	Weight for this service, if any. This weight is used when the system performs load balancing,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			giving greater priority to a specific service. It is useful when the services bound to a virtual server are of different capacity.
cachevserver	<String>	Read-only	The name of the default target cache virtual server, if any, to which requests are redirected.
backupvserver	<String>	Read-only	The name of the backup VPN virtual server for this VPN virtual server.
clttimeout	<Integer>	Read-only	The idle time, if any, in seconds after which the client connection is terminated.
somethod	<String>	Read-only	VPN client applications are allocated from a block of intranet IP addresses. That block may be exhausted after a certain number of connections. This switch specifies the method used to determine whether or not a new connection will spill over, or exhaust,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			the allocated block of intranet IP addresses for that application. Possible values are CONNECTION or DYNAMICCONNECTION. CONNECTION means that a static integer value is the hard limit for the spillover threshold. The spillover threshold is described below. DYNAMICCONNECTION means that the spillover threshold is set according to the maximum number of connections defined for the VPN virtual server. Possible values = CONNECTION, DYNAMICCONNECTION, BANDWIDTH,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			HEALTH, LLMQUOTA, NONE
sothreshold	<Integer>	Read-only	VPN client applications are allocated from a block of intranet IP addresses. That block may be exhausted after a certain number of connections. The value of this option is the number of client connections after which the mapped IP address is used as the client source IP address instead of an address from the allocated block of intranet IP addresses.
sopersistence	<String>	Read-only	Whether or not cookie-based site persistance is enabled for this VPN vserver. Possible values are 'ConnectionProxy', HTTPRedirect, or NONE.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ENABLED, DISABLED
sopersistencetimeout	<Integer>	Read-only	The timeout, if any, for cookie-based site persistance of this VPN vserver.
usemip	<String>	Read-only	Deprecated. See 'map' below. Possible values = ENABLED, DISABLED
map	<String>	Read-only	Whether or not mapped IP addresses are ON or OFF. Mapped IP addresses are source IP addresses for the virtual servers running on the Citrix ADC. Mapped IP addresses are used by the system to connect to the backend servers. Possible values = ON, OFF
bindpoint	<String>	Read-only	Bindpoint to which the policy is bound. Possible values = REQUEST, RESPONSE, ICA_REQUEST,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			OTHERTCP_REQUEST, AAA_REQUEST, AAA_RESPONSE
disableprimaryondown	<String>	Read-only	Tells whether traffic will continue reaching backup virtual servers even after the primary virtual server comes UP from DOWN state. Possible values = ENABLED, DISABLED
secondary	<Boolean>	Read-only	Binds the authentication policy as the secondary policy to use in a two-factor configuration. A user must then authenticate not only via a primary authentication method but also via a secondary authentication method. User groups are aggregated across both. The user name must be exactly the same for both authentication methods, but they can require different passwords.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
groupextraction	<Boolean>	Read-only	Binds the authentication policy to a tertiary chain which will be used only for group extraction. The user will not authenticate against this server, and this will only be called if primary and/or secondary authentication has succeeded.
epaprofileoptional	<Boolean>	Read-only	Mark the EPA profile optional for preauthentication EPA profile. User would be shown a logon page even if the EPA profile fails to evaluate.
ngname	<String>	Read-only	Node group devno to which this authentication virtual sever belongs.
csvserver	<String>	Read-only	Name of the CS vserver to which the VPN vserver is bound.
nodefaultbindings	<String>	Read-only	to determine if the configuration will have default ssl CIPHER and ECC curve bindings. Default value: NO

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = YES, NO
_nextgenapiresource	<String>	Read-only	.
response	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- ENABLE
- DISABLE
- GET (ALL)
- GET
- COUNT
- RENAME
- CHECK

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"vpnvserver":{

<b>"name":<String_value>,

</b><b>"servicetype":<String_value>,

</b>"ipv46":<String_value>,

"range":<Integer_value>,

"port":<Integer_value>,

"ipset":<String_value>,

"state":<String_value>,
```

```
"authentication":<String_value>,

"doublehop":<String_value>,

"maxaaausers":<Integer_value>,

"icaonly":<String_value>,

"icaproxysessionmigration":<String_value>,

"dtls":<String_value>,

"loginonce":<String_value>,

"advancedepa":<String_value>,

"devicecert":<String_value>,

"certkeynames":<String_value>,

"downstateflush":<String_value>,

"listenpolicy":<String_value>,

"listenpriority":<Integer_value>,

"tcpprofilename":<String_value>,

"httpprofilename":<String_value>,

"comment":<String_value>,

"appflowlog":<String_value>,

"icmpvsrresponse":<String_value>,

"rhistate":<String_value>,

"netprofile":<String_value>,

"cginfrahomepageredirect":<String_value>,

"secureprivateaccess":<String_value>,
```

```
"accessrestrictedpageredirect":<String_value>,

"maxloginattempts":<Integer_value>,

"failedlogintimeout":<Integer_value>,

"l2conn":<String_value>,

"deploymenttype":<String_value>,

"rdpserverprofilename":<String_value>,

"windowsepapluginupgrade":<String_value>,

"linuxepapluginupgrade":<String_value>,

"macepapluginupgrade":<String_value>,

"logoutonsmartcardremoval":<String_value>,

"userdomains":<String_value>,

"authnprofile":<String_value>,

"vserverfqdn":<String_value>,

"gslbsitefqdn":<String_value>,

"pcoipvserverprofilename":<String_value>,

"samesite":<String_value>,

"quicprofilename":<String_value>,

"deviceposture":<String_value>,

"wasmmodule":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"vpnvserver":{

<b>"name":<String_value>,

</b>"ipv46":<String_value>,

"ipset":<String_value>,

"authentication":<String_value>,

"doublehop":<String_value>,

"icaonly":<String_value>,

"icaproxysessionmigration":<String_value>,

"dtls":<String_value>,
```

```
"loginonce":<String_value>,

"advancedepa":<String_value>,

"devicecert":<String_value>,

"certkeynames":<String_value>,

"maxaaausers":<Integer_value>,

"downstateflush":<String_value>,

"listenpolicy":<String_value>,

"listenpriority":<Integer_value>,

"tcpprofilename":<String_value>,

"httpprofilename":<String_value>,

"comment":<String_value>,

"appflowlog":<String_value>,

"icmpvsrresponse":<String_value>,

"rhistate":<String_value>,

"netprofile":<String_value>,

"cginfrahomepageredirect":<String_value>,

"secureprivateaccess":<String_value>,

"accessrestrictedpageredirect":<String_value>,

"maxloginattempts":<Integer_value>,

"rdpserverprofilename":<String_value>,

"failedlogintimeout":<Integer_value>,

"l2conn":<String_value>,
```

```
"windowsepapluginupgrade":<String_value>,

"macepapluginupgrade":<String_value>,

"linuxepapluginupgrade":<String_value>,

"logoutonsmartcardremoval":<String_value>,

"userdomains":<String_value>,

"authnprofile":<String_value>,

"vserverfqdn":<String_value>,

"gslbsitefqdn":<String_value>,

"pcoipvserverprofilename":<String_value>,

"samesite":<String_value>,

"quicprofilename":<String_value>,

"deviceposture":<String_value>,

"wasmmodule":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"vpnvserver":{

<b>"name":<String_value>,

</b>"ipset":true,

"authentication":true,

"doublehop":true,

"icaonly":true,

"icaproxysessionmigration":true,

"dtls":true,

"loginonce":true,

"advancedepa":true,

"devicecert":true,

"certkeynames":true,

"maxaaausers":true,

"downstateflush":true,

"listenpolicy":true,

"listenpriority":true,

"tcpprofilename":true,

"httpprofilename":true,

"comment":true,

"appflowlog":true,

"icmpvsrresponse":true,
```

```
"rhistate":true,

"netprofile":true,

"cginfrahomepageredirect":true,

"secureprivateaccess":true,

"accessrestrictedpageredirect":true,

"maxloginattempts":true,

"rdpserverprofilename":true,

"l2conn":true,

"windowsepapluginupgrade":true,

"macepapluginupgrade":true,

"linuxepapluginupgrade":true,

"logoutonsmartcardremoval":true,

"userdomains":true,

"authnprofile":true,

"vserverfqdn":true,

"gslbsitefqdn":true,

"pcoipvserverprofilename":true,

"samesite":true,

"quicprofilename":true,

"deviceposture":true,

"wasmmodule":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

ENABLE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver? **action=enable HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"vpnvserver":{

<b>"name":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DISABLE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver? **action=disable HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"vpnvserver":{

<b>"name":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

RENAME

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver? **action=rename HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"vpnvserver":{

<b>"name":<String_value>,

</b><b>"newname":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

CHECK

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver? **action=check HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"vpnvserver":{

<b>"name":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Payload:

```
{ "vpnvserver": [ {

<b>"name":<String_value>,

</b>"response":<String_value>



}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of vpnvserver resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver? **view=summary**

Use this query-parameter to get the summary output of vpnvserver resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vpnvserver resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vpnvserver": [ {

"name":<String_value>,

"ip":<String_value>,

"ipv46":<String_value>,

"value":<String_value>,

"port":<Integer_value>,
```

```
"range":<Integer_value>,

"ipset":<String_value>,

"servicetype":<String_value>,

"type":<String_value>,

"curstate":<String_value>,

"status":<Integer_value>,

"cachetype":<String_value>,

"redirect":<String_value>,

"precedence":<String_value>,

"redirecturl":<String_value>,

"authentication":<String_value>,

"doublehop":<String_value>,

"icaonly":<String_value>,

"icaproxysessionmigration":<String_value>,

"dtls":<String_value>,

"loginonce":<String_value>,

"advancedepa":<String_value>,

"devicecert":<String_value>,

"certkeynames":<String_value>,

"maxaaausers":<Integer_value>,

"curaaausers":<Integer_value>,

"curtotalusers":<Integer_value>,
```

```
"domain":<String_value>,

"rule":<String_value>,

"policyname":<String_value>,

"servicename":<String_value>,

"weight":<Integer_value>,

"cachevserver":<String_value>,

"backupvserver":<String_value>,

"clttimeout":<Integer_value>,

"somethod":<String_value>,

"sothreshold":<Integer_value>,

"sopersistence":<String_value>,

"sopersistencetimeout":<Integer_value>,

"usemip":<String_value>,

"map":<String_value>,

"downstateflush":<String_value>,

"bindpoint":<String_value>,

"disableprimaryondown":<String_value>,

"listenpolicy":<String_value>,

"listenpriority":<Integer_value>,

"tcpprofilename":<String_value>,

"httpprofilename":<String_value>,

"comment":<String_value>,
```

```
"appflowlog":<String_value>,

"icmpvsrresponse":<String_value>,

"rhistate":<String_value>,

"netprofile":<String_value>,

"cginfrahomepageredirect":<String_value>,

"secureprivateaccess":<String_value>,

"accessrestrictedpageredirect":<String_value>,

"maxloginattempts":<Integer_value>,

"failedlogintimeout":<Integer_value>,

"secondary":<Boolean_value>,

"groupextraction":<Boolean_value>,

"deploymenttype":<String_value>,

"windowsepapluginupgrade":<String_value>,

"linuxepapluginupgrade":<String_value>,

"macepapluginupgrade":<String_value>,

"logoutonsmartcardremoval":<String_value>,

"epaprofileoptional":<Boolean_value>,

"rdpserverprofilename":<String_value>,

"ngname":<String_value>,

"state":<String_value>,

"l2conn":<String_value>,

"userdomains":<String_value>,
```

```
"csvserver":<String_value>,

"authnprofile":<String_value>,

"vserverfqdn":<String_value>,

"gslbsitefqdn":<String_value>,

"pcoipvserverprofilename":<String_value>,

"nodefaultbindings":<String_value>,

"samesite":<String_value>,

"quicprofilename":<String_value>,

"deviceposture":<String_value>,

"wasmmodule":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of vpnvserver resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnvserver": [ {

"name":<String_value>,

"ip":<String_value>,

"ipv46":<String_value>,

"value":<String_value>,

"port":<Integer_value>,

"range":<Integer_value>,

"ipset":<String_value>,

"servicetype":<String_value>,

"type":<String_value>,

"curstate":<String_value>,

"status":<Integer_value>,

"cachetype":<String_value>,

"redirect":<String_value>,
```

```
"precedence":<String_value>,

"redirecturl":<String_value>,

"authentication":<String_value>,

"doublehop":<String_value>,

"icaonly":<String_value>,

"icaproxysessionmigration":<String_value>,

"dtls":<String_value>,

"loginonce":<String_value>,

"advancedepa":<String_value>,

"devicecert":<String_value>,

"certkeynames":<String_value>,

"maxaaausers":<Integer_value>,

"curaaausers":<Integer_value>,

"curtotalusers":<Integer_value>,

"domain":<String_value>,

"rule":<String_value>,

"policyname":<String_value>,

"servicename":<String_value>,

"weight":<Integer_value>,

"cachevserver":<String_value>,

"backupvserver":<String_value>,

"clttimeout":<Integer_value>,
```

```
"somethod":<String_value>,

"sothreshold":<Integer_value>,

"sopersistence":<String_value>,

"sopersistencetimeout":<Integer_value>,

"usemip":<String_value>,

"map":<String_value>,

"downstateflush":<String_value>,

"bindpoint":<String_value>,

"disableprimaryondown":<String_value>,

"listenpolicy":<String_value>,

"listenpriority":<Integer_value>,

"tcpprofilename":<String_value>,

"httpprofilename":<String_value>,

"comment":<String_value>,

"appflowlog":<String_value>,

"icmpvsrresponse":<String_value>,

"rhistate":<String_value>,

"netprofile":<String_value>,

"cginfrahomepageredirect":<String_value>,

"secureprivateaccess":<String_value>,

"accessrestrictedpageredirect":<String_value>,

"maxloginattempts":<Integer_value>,
```

```
"failedlogintimeout":<Integer_value>,

"secondary":<Boolean_value>,

"groupextraction":<Boolean_value>,

"deploymenttype":<String_value>,

"windowsepapluginupgrade":<String_value>,

"linuxepapluginupgrade":<String_value>,

"macepapluginupgrade":<String_value>,

"logoutonsmartcardremoval":<String_value>,

"epaprofileoptional":<Boolean_value>,

"rdpserverprofilename":<String_value>,

"ngname":<String_value>,

"state":<String_value>,

"l2conn":<String_value>,

"userdomains":<String_value>,

"csvserver":<String_value>,

"authnprofile":<String_value>,

"vserverfqdn":<String_value>,

"gslbsitefqdn":<String_value>,

"pcoipvserverprofilename":<String_value>,

"nodefaultbindings":<String_value>,

"samesite":<String_value>,

"quicprofilename":<String_value>,
```

```
"deviceposture":<String_value>,

"wasmmodule":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vpnvserver": [ { "__count": "#no"} ] }
```

vpnvserver_aaapreauthenticationpolicy_binding

Binding object showing the aaapreauthenticationpolicy that can be bound to vpnvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
gotopriorityexpression	<String>	Read-write	Applicable only to advance vpn session policy. Expression or other value specifying the next policy to evaluate if the current policy evaluates to TRUE. Specify one of the following values: * NEXT - Evaluate the policy with the next higher priority number. * END - End policy evaluation. * An expression that evaluates to a number. If you specify an expression, the number to which it evaluates determines the next policy to evaluate, as follows: * If the expression evaluates to a higher numbered priority, the policy with that priority is evaluated next. * If the expression evaluates to the priority of the current policy, the policy with the next higher numbered priority is evaluated next. * If the expression evaluates to a number that is larger than the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			largest numbered priority, policy evaluation ends. An UNDEF event is triggered if: * The expression is invalid. * The expression evaluates to a priority number that is numerically lower than the current policy's priority. * The expression evaluates to a priority number that is between the current policy's priority number (say, 30) and the highest priority number (say, 100), but does not match any configured priority number (for example, the expression evaluates to the number 85). This example assumes that the priority number increments by 10 for every successive policy, and therefore a priority number of 85 does not exist in the policy label.
policy	<String>	Read-write	The name of the policy, if any, bound to the VPN virtual server.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
groupextraction	<Boolean>	Read-write	Binds the authentication policy to a tertiary chain which will be used only for group extraction. The user will not authenticate against this server, and this will only be called if primary and/or secondary authentication has succeeded.
bindpoint	<String>	Read-write	Bind point to which to bind the policy. Applies only to rewrite and cache policies. If you do not set this parameter, the policy is bound to REQ_DEFAULT or RES_DEFAULT, depending on whether the policy rule is a response-time or a request-time expression. Possible values = REQUEST, RESPONSE, ICA_REQUEST, OTHERTCP_REQUEST, AAA_REQUEST, AAA_RESPONSE
priority	<Integer>	Read-write	Integer specifying the policy's priority. The lower the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			number, the higher the priority. Policies are evaluated in the order of their priority numbers. Maximum value for default syntax policies is 2147483647 and for classic policies is 64000. Minimum value = 0 Maximum value = 2147483647
name	<String>	Read-write	Name of the virtual server. Minimum length = 1
secondary	<Boolean>	Read-write	Binds the authentication policy as the secondary policy to use in a two-factor configuration. A user must then authenticate not only via a primary authentication method but also via a secondary authentication method. User groups are aggregated across both. The user name must be exactly the same for both authentication methods, but they can require different passwords.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
acttype	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/vpnvserver_aaapreauthenticationpolicy_binding
HTTP Method: PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"vpnvserver_aaapreauthenticationpolicy_binding":{

<b>"name":<String_value>,

</b>"policy":<String_value>,

"priority":<Integer_value>,

"secondary":<Boolean_value>,

"groupextraction":<Boolean_value>,

"gotopriorityexpression":<String_value>,

"bindpoint":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_aaapreauthenticationpolicy_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_aaapreauthenticationpolicy_binding/ name_value<String> ? **args=policy: <String_value> ,secondary: <Boolean_value> ,groupextraction: <Boolean_value> ,bindpoint: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_aaapreauthenticationpolicy_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_aaapreauthenticationpolicy_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of vpnvserver_aaapreauthenticationpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_aaapreauthenticationpolicy_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vpnvserver_aaapreauthenticationpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnvserver_aaapreauthenticationpolicy_binding": [ {

"gotopriorityexpression":<String_value>,

"policy":<String_value>,

"groupextraction":<Boolean_value>,

"bindpoint":<String_value>,

"priority":<Integer_value>,

"name":<String_value>,

"secondary":<Boolean_value>,

"acttype":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_aaapreauthenticationpolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_aaapreauthenticationpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnvserver_aaapreauthenticationpolicy_binding": [ {

"gotopriorityexpression":<String_value>,

"policy":<String_value>,

"groupextraction":<Boolean_value>,

"bindpoint":<String_value>,

"priority":<Integer_value>,

"name":<String_value>,

"secondary":<Boolean_value>,

"acttype":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_aaapreauthenticationpolicy_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"vpnvserver_aaapreauthenticationpolicy_binding": [ { "__count":
"#no"} ] }
```

vpnvserver_analyticsprofile_binding

Binding object showing the analyticsprofile that can be bound to vpnvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the virtual server. Minimum length = 1
analyticsprofile	<String>	Read-write	Name of the analytics profile bound to the VPN Vserver.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/vpnvserver_analyticsprofile_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"vpnvserver_analyticsprofile_binding":{

<b>"name":<String_value>,

</b>"analyticsprofile":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_analyticsprofile_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_analyticsprofile_binding/ name_value<String> ? **args=analyticsprofile: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_analyticsprofile_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_analyticsprofile_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of vpnvserver_analyticsprofile_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_analyticsprofile_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vpnvserver_analyticsprofile_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnvserver_analyticsprofile_binding": [ {

"name":<String_value>,

"analyticsprofile":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_analyticsprofile_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_analyticsprofile_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnvserver_analyticsprofile_binding": [ {

"name":<String_value>,

"analyticsprofile":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_analyticsprofile_binding/name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"vpnvserver_analyticsprofile_binding": [ { "__count": "#no"} ] }
```

vpnvserver_appcontroller_binding

Binding object showing the appcontroller that can be bound to vpnvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
appcontroller	<String>	Read-write	Configured App Controller server in XenMobile deployment.
name	<String>	Read-write	Name of the virtual server. Minimum length = 1
acttype	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/vpnvserver_appcontroller_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"vpnvserver_appcontroller_binding":{

<b>"name":<String_value>,
```

```
</b>"appcontroller":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_appcontroller_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_appcontroller_binding/ name_value<String> ? **args=appcontroller: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_appcontroller_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_appcontroller_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of vpnvserver_appcontroller_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_appcontroller_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vpnvserver_appcontroller_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnvserver_appcontroller_binding": [ {

"appcontroller":<String_value>,

"name":<String_value>,

"acttype":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_appcontroller_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_appcontroller_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnvserver_appcontroller_binding": [ {

"appcontroller":<String_value>,

"name":<String_value>,

"acttype":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_appcontroller_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"vpnvserver_appcontroller_binding": [ { "__count": "#no"} ] }
```

vpnvserver_appflowpolicy_binding

Binding object showing the appflowpolicy that can be bound to vpnvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
gotopriorityexpression	<String>	Read-write	Next priority expression.
policy	<String>	Read-write	The name of the policy, if any, bound to the VPN virtual server.
groupextraction	<Boolean>	Read-write	Binds the authentication policy to a tertiary chain which will be used only for group extraction. The user will not authenticate against this server, and this will only be called if primary and/or secondary authentication has succeeded.
bindpoint	<String>	Read-write	Bindpoint to which the policy is bound. Possible values = REQUEST, RESPONSE, ICA_REQUEST, OTHERTCP_REQUEST, AAA_REQUEST, AAA_RESPONSE

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
priority	<Integer>	Read-write	Integer specifying the policy's priority. The lower the number, the higher the priority. Policies are evaluated in the order of their priority numbers. Maximum value for default syntax policies is 2147483647 and for classic policies is 64000. Minimum value = 0 Maximum value = 2147483647
name	<String>	Read-write	Name of the virtual server. Minimum length = 1
secondary	<Boolean>	Read-write	Binds the authentication policy as the secondary policy to use in a two-factor configuration. A user must then authenticate not only via a primary authentication method but also via a secondary authentication method. User groups are aggregated across both. The user name must be exactly the same for both authentication

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			methods, but they can require different passwords.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/vpnvserver_appflowpolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"vpnvserver_appflowpolicy_binding":{

<b>"name":<String_value>,

</b>"policy":<String_value>,

"priority":<Integer_value>,

"secondary":<Boolean_value>,

"groupextraction":<Boolean_value>,

"gotopriorityexpression":<String_value>,

"bindpoint":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_appflowpolicy_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_appflowpolicy_binding/ name_value<String> ? **args=policy: <String_value> ,secondary: <Boolean_value> ,groupextraction: <Boolean_value> ,bindpoint: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_appflowpolicy_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_appflowpolicy_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of vpnvserver_appflowpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_appflowpolicy_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vpnvserver_appflowpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnvserver_appflowpolicy_binding": [ {

"gotopriorityexpression":<String_value>,

"policy":<String_value>,

"groupextraction":<Boolean_value>,

"bindpoint":<String_value>,

"priority":<Integer_value>,

"name":<String_value>,

"secondary":<Boolean_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_appflowpolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_appflowpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnvserver_appflowpolicy_binding": [ {

"gotopriorityexpression":<String_value>,

"policy":<String_value>,

"groupextraction":<Boolean_value>,

"bindpoint":<String_value>,

"priority":<Integer_value>,

"name":<String_value>,

"secondary":<Boolean_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_appflowpolicy_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"vpnvserver_appflowpolicy_binding": [ { "__count": "#no"} ] }
```

vpnvserver_appfwpolicy_binding

Binding object showing the appfwpolicy that can be bound to vpnvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
priority	<Integer>	Read-write	Integer specifying the policy's priority. The lower the number, the higher the priority. Policies are evaluated in the order of their priority numbers. Maximum value for default syntax policies is 2147483647 and for classic policies is 64000. Minimum value = 0 Maximum value = 2147483647
bindpoint	<String>	Read-write	Bind point to which to bind the policy. Applies only to rewrite and cache policies. If you do not set this parameter, the policy is bound to

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			REQ_DEFAULT or RES_DEFAULT, depending on whether the policy rule is a response-time or a request-time expression. Possible values = REQUEST, RESPONSE, ICA_REQUEST, OTHERTCP_REQUEST, AAA_REQUEST, AAA_RESPONSE
name	<String>	Read-write	Name of the virtual server. Minimum length = 1
secondary	<Boolean>	Read-write	Binds the authentication policy as the secondary policy to use in a two-factor configuration. A user must then authenticate not only via a primary authentication method but also via a secondary authentication method. User groups are aggregated across both. The user name must be exactly the same for both authentication methods, but they

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			can require different passwords.
gotopriorityexpression	<String>	Read-write	Next priority expression.
policy	<String>	Read-write	The name of the policy, if any, bound to the VPN virtual server.
groupextraction	<Boolean>	Read-write	Binds the authentication policy to a tertiary chain which will be used only for group extraction. The user will not authenticate against this server, and this will only be called if primary and/or secondary authentication has succeeded.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/vpnvserver_appfwpolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"vpnvserver_appfwpolicy_binding":{

<b>"name":<String_value>,
```

```
</b>"policy":<String_value>,

"priority":<Integer_value>,

"secondary":<Boolean_value>,

"groupextraction":<Boolean_value>,

"gotopriorityexpression":<String_value>,

"bindpoint":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_appfwpolicy_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_appfwpolicy_binding/ name_value<String> ? **args=policy: <String_value> ,secondary: <Boolean_value> ,groupextraction: <Boolean_value> ,bindpoint: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_appfwpolicy_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/

vpnvserver_appfwpolicy_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of vpnvserver_appfwpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_appfwpolicy_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vpnvserver_appfwpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnvserver_appfwpolicy_binding": [ {

"priority":<Integer_value>,

"bindpoint":<String_value>,

"name":<String_value>,

"secondary":<Boolean_value>,

"gotopriorityexpression":<String_value>,

"policy":<String_value>,
```

```
"groupextraction":<Boolean_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_appfwpolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_appfwpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnvserver_appfwpolicy_binding": [ {

"priority":<Integer_value>,

"bindpoint":<String_value>,

"name":<String_value>,

"secondary":<Boolean_value>,
```

```
"gotopriorityexpression":<String_value>,

"policy":<String_value>,

"groupextraction":<Boolean_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_appfwpolicy_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"vpnvserver_appfwpolicy_binding": [ { "__count": "#no"} ] }
```

vpnvserver_auditnslogpolicy_binding

Binding object showing the auditnslogpolicy that can be bound to vpnvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
groupextraction	<Boolean>	Read-write	Binds the authentication policy to a tertiary chain which will be used only for group extraction. The user will not authenticate against this server, and this will only be called if primary and/or secondary authentication has succeeded.
policy	<String>	Read-write	The name of the policy, if any, bound to the VPN virtual server.
gotopriorityexpression	<String>	Read-write	Applicable only to advance vpn session policy. Expression or other value specifying the next policy to evaluate if the current policy evaluates to TRUE. Specify one of the following values: * NEXT - Evaluate the policy with the next higher priority number. * END - End policy evaluation. * An expression that evaluates to a number. If you specify an expression, the number to which it evaluates

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			determines the next policy to evaluate, as follows: * If the expression evaluates to a higher numbered priority, the policy with that priority is evaluated next. * If the expression evaluates to the priority of the current policy, the policy with the next higher numbered priority is evaluated next. * If the expression evaluates to a number that is larger than the largest numbered priority, policy evaluation ends. An UNDEF event is triggered if: * The expression is invalid. * The expression evaluates to a priority number that is numerically lower than the current policy's priority. * The expression evaluates to a priority number that is between the current policy's priority number (say, 30) and the highest priority number (say, 100), but does not match any configured priority

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			number (for example, the expression evaluates to the number 85). This example assumes that the priority number increments by 10 for every successive policy, and therefore a priority number of 85 does not exist in the policy label.
priority	<Integer>	Read-write	Integer specifying the policy's priority. The lower the number, the higher the priority. Policies are evaluated in the order of their priority numbers. Maximum value for default syntax policies is 2147483647 and for classic policies is 64000. Minimum value = 0 Maximum value = 2147483647
bindpoint	<String>	Read-write	Bind point to which to bind the policy. Applies only to rewrite and cache policies. If you do not set this parameter, the policy is bound to REQ_DEFAULT or RES_DEFAULT,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			depending on whether the policy rule is a response-time or a request-time expression. Possible values = REQUEST, RESPONSE, ICA_REQUEST, OTHERTCP_REQUEST, AAA_REQUEST, AAA_RESPONSE
secondary	<Boolean>	Read-write	Binds the authentication policy as the secondary policy to use in a two-factor configuration. A user must then authenticate not only via a primary authentication method but also via a secondary authentication method. User groups are aggregated across both. The user name must be exactly the same for both authentication methods, but they can require different passwords.
name	<String>	Read-write	Name of the virtual server.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum length = 1
acttype	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/vpnvserver_auditnslogpolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"vpnvserver_auditnslogpolicy_binding":{

<b>"name":<String_value>,

</b>"policy":<String_value>,

"priority":<Integer_value>,

"secondary":<Boolean_value>,

"groupextraction":<Boolean_value>,

"gotopriorityexpression":<String_value>,

"bindpoint":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_auditnslogpolicy_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_auditnslogpolicy_binding/ name_value<String> ? **args=policy: <String_value> ,secondary: <Boolean_value> ,groupextraction: <Boolean_value> ,bindpoint: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_auditnslogpolicy_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_auditnslogpolicy_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of vpnvserver_auditnslogpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_auditnslogpolicy_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vpnvserver_auditnslogpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnvserver_auditnslogpolicy_binding": [ {

"groupextraction":<Boolean_value>,

"policy":<String_value>,

"gotopriorityexpression":<String_value>,

"priority":<Integer_value>,

"bindpoint":<String_value>,

"secondary":<Boolean_value>,

"name":<String_value>,

"acttype":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_auditnslogpolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_auditnslogpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnvserver_auditnslogpolicy_binding": [ {

"groupextraction":<Boolean_value>,

"policy":<String_value>,

"gotopriorityexpression":<String_value>,

"priority":<Integer_value>,

"bindpoint":<String_value>,

"secondary":<Boolean_value>,

"name":<String_value>,

"acttype":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_auditnslogpolicy_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"vpnvserver_auditnslogpolicy_binding": [ { "__count": "#no"} ] }
```

vpnvserver_auditsyslogpolicy_binding

Binding object showing the auditsyslogpolicy that can be bound to vpnvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
bindpoint	<String>	Read-write	Bind point to which to bind the policy. Applies only to rewrite and cache policies. If you do not set this parameter, the policy is bound to REQ_DEFAULT or RES_DEFAULT, depending on whether the policy rule is a response-time or a request-time expression. Possible values = REQUEST, RESPONSE, ICA_REQUEST, OTHERTCP_REQUEST,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			AAA_REQUEST, AAA_RESPONSE
priority	<Integer>	Read-write	Integer specifying the policy's priority. The lower the number, the higher the priority. Policies are evaluated in the order of their priority numbers. Maximum value for default syntax policies is 2147483647 and for classic policies is 64000. Minimum value = 0 Maximum value = 2147483647
name	<String>	Read-write	Name of the virtual server. Minimum length = 1
secondary	<Boolean>	Read-write	Binds the authentication policy as the secondary policy to use in a two-factor configuration. A user must then authenticate not only via a primary authentication method but also via a secondary authentication method. User groups are aggregated across both. The

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			user name must be exactly the same for both authentication methods, but they can require different passwords.
gotopriorityexpression	<String>	Read-write	Applicable only to advance vpn session policy. Expression or other value specifying the next policy to evaluate if the current policy evaluates to TRUE. Specify one of the following values: * NEXT - Evaluate the policy with the next higher priority number. * END - End policy evaluation. * An expression that evaluates to a number. If you specify an expression, the number to which it evaluates determines the next policy to evaluate, as follows: * If the expression evaluates to a higher numbered priority, the policy with that priority is evaluated next. * If the expression evaluates to the priority of the current policy, the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			policy with the next higher numbered priority is evaluated next. * If the expression evaluates to a number that is larger than the largest numbered priority, policy evaluation ends. An UNDEF event is triggered if: * The expression is invalid. * The expression evaluates to a priority number that is numerically lower than the current policy's priority. * The expression evaluates to a priority number that is between the current policy's priority number (say, 30) and the highest priority number (say, 100), but does not match any configured priority number (for example, the expression evaluates to the number 85). This example assumes that the priority number increments by 10 for every successive policy, and therefore a priority number of

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			85 does not exist in the policy label.
policy	<String>	Read-write	The name of the policy, if any, bound to the VPN virtual server.
groupextraction	<Boolean>	Read-write	Binds the authentication policy to a tertiary chain which will be used only for group extraction. The user will not authenticate against this server, and this will only be called if primary and/or secondary authentication has succeeded.
acttype	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/vpnvserver_auditsyslogpolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"vpnvserver_auditsyslogpolicy_binding":{

<b>"name":<String_value>,
```

```
</b>"policy":<String_value>,

"priority":<Integer_value>,

"secondary":<Boolean_value>,

"groupextraction":<Boolean_value>,

"gotopriorityexpression":<String_value>,

"bindpoint":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_auditsyslogpolicy_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_auditsyslogpolicy_binding/ name_value<String> ? **args=policy: <String_value> ,secondary: <Boolean_value> ,groupextraction: <Boolean_value> ,bindpoint: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_auditsyslogpolicy_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/

vpnvserver_auditsyslogpolicy_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of vpnvserver_auditsyslogpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_auditsyslogpolicy_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vpnvserver_auditsyslogpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnvserver_auditsyslogpolicy_binding": [ {

"bindpoint":<String_value>,

"priority":<Integer_value>,

"name":<String_value>,

"secondary":<Boolean_value>,

"gotopriorityexpression":<String_value>,

"policy":<String_value>,
```

```
"groupextraction":<Boolean_value>,

"acttype":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_auditsyslogpolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_auditsyslogpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnvserver_auditsyslogpolicy_binding": [ {

"bindpoint":<String_value>,

"priority":<Integer_value>,

"name":<String_value>,
```

```
"secondary":<Boolean_value>,

"gotopriorityexpression":<String_value>,

"policy":<String_value>,

"groupextraction":<Boolean_value>,

"acttype":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_auditsyslogpolicy_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"vpnvserver_auditsyslogpolicy_binding": [ { "__count": "#no"} ] }
```

vpnvserver_authenticationcertpolicy_binding

Binding object showing the authenticationcertpolicy that can be bound to vpnvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
bindpoint	<String>	Read-write	Bind point to which to bind the policy. Applies only to rewrite and cache policies. If you do not set this parameter, the policy is bound to REQ_DEFAULT or RES_DEFAULT, depending on whether the policy rule is a response-time or a request-time expression. Possible values = REQUEST, RESPONSE, ICA_REQUEST, OTHERTCP_REQUEST, AAA_REQUEST, AAA_RESPONSE
priority	<Integer>	Read-write	Integer specifying the policy's priority. The lower the number, the higher the priority. Policies are evaluated in the order of their priority numbers. Maximum value for default syntax policies is 2147483647 and for classic policies is 64000.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum value = 0 Maximum value = 2147483647
secondary	<Boolean>	Read-write	Binds the authentication policy as the secondary policy to use in a two-factor configuration. A user must then authenticate not only via a primary authentication method but also via a secondary authentication method. User groups are aggregated across both. The user name must be exactly the same for both authentication methods, but they can require different passwords.
name	<String>	Read-write	Name of the virtual server. Minimum length = 1
policy	<String>	Read-write	The name of the policy, if any, bound to the VPN virtual server.
gotopriorityexpression	<String>	Read-write	Applicable only to advance vpn session policy. Expression or other value

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			specifying the next policy to evaluate if the current policy evaluates to TRUE. Specify one of the following values: * NEXT - Evaluate the policy with the next higher priority number. * END - End policy evaluation. * An expression that evaluates to a number. If you specify an expression, the number to which it evaluates determines the next policy to evaluate, as follows: * If the expression evaluates to a higher numbered priority, the policy with that priority is evaluated next. * If the expression evaluates to the priority of the current policy, the policy with the next higher numbered priority is evaluated next. * If the expression evaluates to a number that is larger than the largest numbered priority, policy evaluation ends. An UNDEF event is

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			triggered if: * The expression is invalid. * The expression evaluates to a priority number that is numerically lower than the current policy's priority. * The expression evaluates to a priority number that is between the current policy's priority number (say, 30) and the highest priority number (say, 100), but does not match any configured priority number (for example, the expression evaluates to the number 85). This example assumes that the priority number increments by 10 for every successive policy, and therefore a priority number of 85 does not exist in the policy label.
groupextraction	<Boolean>	Read-write	Binds the authentication policy to a tertiary chain which will be used only for group extraction. The user will not authenticate against this server, and this will only be

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			called if primary and/ or secondary authentication has succeeded.
acttype	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/vpnvserver_authenticationcertpolicy_binding
HTTP Method: PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"vpnvserver_authenticationcertpolicy_binding":{

<b>"name":<String_value>,

</b>"policy":<String_value>,

"priority":<Integer_value>,

"secondary":<Boolean_value>,

"groupextraction":<Boolean_value>,

"gotopriorityexpression":<String_value>,

"bindpoint":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_authenticationcertpolicy_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_authenticationcertpolicy_binding/ name_value<String> ? **args=policy: <String_value> ,secondary: <Boolean_value> ,groupextraction: <Boolean_value> ,bindpoint: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_authenticationcertpolicy_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_authenticationcertpolicy_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of vpnvserver_authenticationcertpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_authenticationcertpolicy_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vpnvserver_authenticationcertpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnvserver_authenticationcertpolicy_binding": [ {

"bindpoint":<String_value>,

"priority":<Integer_value>,

"secondary":<Boolean_value>,

"name":<String_value>,

"policy":<String_value>,

"gotopriorityexpression":<String_value>,

"groupextraction":<Boolean_value>,

"acttype":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_authenticationcertpolicy_binding
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_authenticationcertpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnvserver_authenticationcertpolicy_binding": [ {

"bindpoint":<String_value>,

"priority":<Integer_value>,

"secondary":<Boolean_value>,

"name":<String_value>,

"policy":<String_value>,

"gotopriorityexpression":<String_value>,

"groupextraction":<Boolean_value>,

"acttype":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_authenticationcertpolicy_binding/name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"vpnvserver_authenticationcertpolicy_binding": [ { "__count": "#no"} ] }
```

vpnvserver_authenticationdfapolicy_binding

Binding object showing the authenticationdfapolicy that can be bound to vpnvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
groupextraction	<Boolean>	Read-write	Binds the authentication policy to a tertiary chain which will be used only for group extraction. The user will not authenticate against this server, and this will only be called if primary and/or secondary authentication has succeeded.
policy	<String>	Read-write	The name of the policy, if any, bound to the VPN virtual server.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
gotopriorityexpression	<String>	Read-write	Applicable only to advance vpn session policy. Expression or other value specifying the next policy to evaluate if the current policy evaluates to TRUE. Specify one of the following values: * NEXT - Evaluate the policy with the next higher priority number. * END - End policy evaluation. * An expression that evaluates to a number. If you specify an expression, the number to which it evaluates determines the next policy to evaluate, as follows: * If the expression evaluates to a higher numbered priority, the policy with that priority is evaluated next. * If the expression evaluates to the priority of the current policy, the policy with the next higher numbered priority is evaluated next. * If the expression evaluates to a number that is larger than the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			largest numbered priority, policy evaluation ends. An UNDEF event is triggered if: * The expression is invalid. * The expression evaluates to a priority number that is numerically lower than the current policy's priority. * The expression evaluates to a priority number that is between the current policy's priority number (say, 30) and the highest priority number (say, 100), but does not match any configured priority number (for example, the expression evaluates to the number 85). This example assumes that the priority number increments by 10 for every successive policy, and therefore a priority number of 85 does not exist in the policy label.
secondary	<Boolean>	Read-write	Binds the authentication policy as the secondary policy to use in a two-factor

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			configuration. A user must then authenticate not only via a primary authentication method but also via a secondary authentication method. User groups are aggregated across both. The user name must be exactly the same for both authentication methods, but they can require different passwords.
name	<String>	Read-write	Name of the virtual server. Minimum length = 1
bindpoint	<String>	Read-write	Bind point to which to bind the policy. Applies only to rewrite and cache policies. If you do not set this parameter, the policy is bound to REQ_DEFAULT or RES_DEFAULT, depending on whether the policy rule is a response-time or a request-time expression. Possible values = REQUEST, RESPONSE, ICA_REQUEST,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			OTHERTCP_REQUEST, AAA_REQUEST, AAA_RESPONSE
priority	<Integer>	Read-write	Integer specifying the policy's priority. The lower the number, the higher the priority. Policies are evaluated in the order of their priority numbers. Maximum value for default syntax policies is 2147483647 and for classic policies is 64000. Minimum value = 0 Maximum value = 2147483647
acttype	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/vpnvserver_authenticationdfapolicy_binding
HTTP Method: PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"vpnvserver_authenticationdfapolicy_binding":{

<b>"name":<String_value>,
```

```
</b>"policy":<String_value>,

"priority":<Integer_value>,

"secondary":<Boolean_value>,

"groupextraction":<Boolean_value>,

"gotopriorityexpression":<String_value>,

"bindpoint":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_authenticationdfapolicy_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_authenticationdfapolicy_binding/ name_value<String> ? **args=policy: <String_value> ,secondary: <Boolean_value> ,groupextraction: <Boolean_value> ,bindpoint: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_authenticationdfapolicy_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/

vpnvserver_authenticationdfapolicy_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of vpnvserver_authenticationdfapolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_authenticationdfapolicy_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vpnvserver_authenticationdfapolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnvserver_authenticationdfapolicy_binding": [ {

"groupextraction":<Boolean_value>,

"policy":<String_value>,

"gotopriorityexpression":<String_value>,

"secondary":<Boolean_value>,

"name":<String_value>,

"bindpoint":<String_value>,
```

```
"priority":<Integer_value>,

"acttype":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_authenticationdfapolicy_binding
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_authenticationdfapolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnvserver_authenticationdfapolicy_binding": [ {

"groupextraction":<Boolean_value>,

"policy":<String_value>,

"gotopriorityexpression":<String_value>,
```

```
"secondary":<Boolean_value>,

"name":<String_value>,

"bindpoint":<String_value>,

"priority":<Integer_value>,

"acttype":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_authenticationdfapolicy_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"vpnvserver_authenticationdfapolicy_binding": [ { "__count": "#no"} ] }
```

vpnvserver_authenticationldappolicy_binding

Binding object showing the authenticationldappolicy that can be bound to vpnvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
policy	<String>	Read-write	The name of the policy, if any, bound to the VPN virtual server.
gotopriorityexpression	<String>	Read-write	Applicable only to advance vpn session policy. Expression or other value specifying the next policy to evaluate if the current policy evaluates to TRUE. Specify one of the following values: * NEXT - Evaluate the policy with the next higher priority number. * END - End policy evaluation. * An expression that evaluates to a number. If you specify an expression, the number to which it evaluates determines the next policy to evaluate, as follows: * If the expression evaluates to a higher numbered priority, the policy with that priority is evaluated next. * If the expression evaluates to the priority of the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			current policy, the policy with the next higher numbered priority is evaluated next. * If the expression evaluates to a number that is larger than the largest numbered priority, policy evaluation ends. An UNDEF event is triggered if: * The expression is invalid. * The expression evaluates to a priority number that is numerically lower than the current policy's priority. * The expression evaluates to a priority number that is between the current policy's priority number (say, 30) and the highest priority number (say, 100), but does not match any configured priority number (for example, the expression evaluates to the number 85). This example assumes that the priority number increments by 10 for every successive policy, and therefore a priority number of

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			85 does not exist in the policy label.
groupextraction	<Boolean>	Read-write	Binds the authentication policy to a tertiary chain which will be used only for group extraction. The user will not authenticate against this server, and this will only be called if primary and/or secondary authentication has succeeded.
bindpoint	<String>	Read-write	Bind point to which to bind the policy. Applies only to rewrite and cache policies. If you do not set this parameter, the policy is bound to REQ_DEFAULT or RES_DEFAULT, depending on whether the policy rule is a response-time or a request-time expression. Possible values = REQUEST, RESPONSE, ICA_REQUEST, OTHERTCP_REQUEST, AAA_REQUEST, AAA_RESPONSE

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
priority	<Integer>	Read-write	Integer specifying the policy's priority. The lower the number, the higher the priority. Policies are evaluated in the order of their priority numbers. Maximum value for default syntax policies is 2147483647 and for classic policies is 64000. Minimum value = 0 Maximum value = 2147483647
secondary	<Boolean>	Read-write	Binds the authentication policy as the secondary policy to use in a two-factor configuration. A user must then authenticate not only via a primary authentication method but also via a secondary authentication method. User groups are aggregated across both. The user name must be exactly the same for both authentication methods, but they can require different passwords.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the virtual server. Minimum length = 1
acttype	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/vpnvserver_authenticationldappolicy_binding
HTTP Method: PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"vpnvserver_authenticationldappolicy_binding":{

<b>"name":<String_value>,

</b>"policy":<String_value>,

"priority":<Integer_value>,

"secondary":<Boolean_value>,

"groupextraction":<Boolean_value>,

"gotopriorityexpression":<String_value>,

"bindpoint":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_authenticationldappolicy_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_authenticationldappolicy_binding/ name_value<String> ? **args=policy: <String_value> ,secondary: <Boolean_value> ,groupextraction: <Boolean_value> ,bindpoint: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_authenticationldappolicy_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_authenticationldappolicy_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of vpnvserver_authenticationldappolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_authenticationldappolicy_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vpnvserver_authenticationldappolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnvserver_authenticationldappolicy_binding": [ {

"policy":<String_value>,

"gotopriorityexpression":<String_value>,

"groupextraction":<Boolean_value>,

"bindpoint":<String_value>,

"priority":<Integer_value>,

"secondary":<Boolean_value>,

"name":<String_value>,

"acttype":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_authenticationldappolicy_binding
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_authenticationldappolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnvserver_authenticationldappolicy_binding": [ {

"policy":<String_value>,

"gotopriorityexpression":<String_value>,

"groupextraction":<Boolean_value>,

"bindpoint":<String_value>,

"priority":<Integer_value>,

"secondary":<Boolean_value>,

"name":<String_value>,

"acttype":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_authenticationldappolicy_binding/name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"vpnvserver_authenticationldappolicy_binding": [ { "__count": "#no"} ] }
```

vpnvserver_authenticationlocalpolicy_binding

Binding object showing the authenticationlocalpolicy that can be bound to vpnvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
groupextraction	<Boolean>	Read-write	Binds the authentication policy to a tertiary chain which will be used only for group extraction. The user will not authenticate against this server, and this will only be called if primary and/or secondary authentication has succeeded.
gotopriorityexpression	<String>	Read-write	Applicable only to advance vpn session policy. Expression or other value

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			specifying the next policy to evaluate if the current policy evaluates to TRUE. Specify one of the following values: * NEXT - Evaluate the policy with the next higher priority number. * END - End policy evaluation. * An expression that evaluates to a number. If you specify an expression, the number to which it evaluates determines the next policy to evaluate, as follows: * If the expression evaluates to a higher numbered priority, the policy with that priority is evaluated next. * If the expression evaluates to the priority of the current policy, the policy with the next higher numbered priority is evaluated next. * If the expression evaluates to a number that is larger than the largest numbered priority, policy evaluation ends. An UNDEF event is

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			triggered if: * The expression is invalid. * The expression evaluates to a priority number that is numerically lower than the current policy's priority. * The expression evaluates to a priority number that is between the current policy's priority number (say, 30) and the highest priority number (say, 100), but does not match any configured priority number (for example, the expression evaluates to the number 85). This example assumes that the priority number increments by 10 for every successive policy, and therefore a priority number of 85 does not exist in the policy label.
policy	<String>	Read-write	The name of the policy, if any, bound to the VPN virtual server.
bindpoint	<String>	Read-write	Bind point to which to bind the policy. Applies only to rewrite and cache

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			policies. If you do not set this parameter, the policy is bound to REQ_DEFAULT or RES_DEFAULT, depending on whether the policy rule is a response-time or a request-time expression. Possible values = REQUEST, RESPONSE, ICA_REQUEST, OTHERTCP_REQUEST, AAA_REQUEST, AAA_RESPONSE
priority	<Integer>	Read-write	Integer specifying the policy's priority. The lower the number, the higher the priority. Policies are evaluated in the order of their priority numbers. Maximum value for default syntax policies is 2147483647 and for classic policies is 64000. Minimum value = 0 Maximum value = 2147483647
name	<String>	Read-write	Name of the virtual server.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum length = 1
secondary	<Boolean>	Read-write	Binds the authentication policy as the secondary policy to use in a two-factor configuration. A user must then authenticate not only via a primary authentication method but also via a secondary authentication method. User groups are aggregated across both. The user name must be exactly the same for both authentication methods, but they can require different passwords.
acttype	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/vpnvserver_authenticationlocalpolicy_binding
HTTP Method: PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"vpnvserver_authenticationlocalpolicy_binding":{

<b>"name":<String_value>,
```

```
</b>"policy":<String_value>,

"priority":<Integer_value>,

"secondary":<Boolean_value>,

"groupextraction":<Boolean_value>,

"gotopriorityexpression":<String_value>,

"bindpoint":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_authenticationlocalpolicy_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_authenticationlocalpolicy_binding/ name_value<String> ? **args=policy: <String_value> ,secondary: <Boolean_value> ,groupextraction: <Boolean_value> ,bindpoint: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_authenticationlocalpolicy_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/

vpnvserver_authenticationlocalpolicy_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of vpnvserver_authenticationlocalpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_authenticationlocalpolicy_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vpnvserver_authenticationlocalpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnvserver_authenticationlocalpolicy_binding": [ {

"groupextraction":<Boolean_value>,

"gotopriorityexpression":<String_value>,

"policy":<String_value>,

"bindpoint":<String_value>,

"priority":<Integer_value>,

"name":<String_value>,
```

```
"secondary":<Boolean_value>,

"acttype":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_authenticationlocalpolicy_binding
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_authenticationlocalpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnvserver_authenticationlocalpolicy_binding": [ {

"groupextraction":<Boolean_value>,

"gotopriorityexpression":<String_value>,

"policy":<String_value>,
```

```
"bindpoint":<String_value>,

"priority":<Integer_value>,

"name":<String_value>,

"secondary":<Boolean_value>,

"acttype":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_authenticationlocalpolicy_binding/name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"vpnvserver_authenticationlocalpolicy_binding": [ { "__count": "#no"} ] }
```

vpnvserver_authenticationloginschemapolicy_binding

Binding object showing the authenticationloginschemapolicy that can be bound to vpnvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
gotopriorityexpression	<String>	Read-write	Next priority expression.
policy	<String>	Read-write	The name of the policy, if any, bound to the VPN virtual server.
groupextraction	<Boolean>	Read-write	Binds the authentication policy to a tertiary chain which will be used only for group extraction. The user will not authenticate against this server, and this will only be called if primary and/or secondary authentication has succeeded.
name	<String>	Read-write	Name of the virtual server. Minimum length = 1
secondary	<Boolean>	Read-write	Binds the authentication policy as the secondary policy to use in a two-factor configuration. A user must then authenticate not only via a primary authentication method but also via a secondary

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			authentication method. User groups are aggregated across both. The user name must be exactly the same for both authentication methods, but they can require different passwords.
priority	<Integer>	Read-write	Integer specifying the policy's priority. The lower the number, the higher the priority. Policies are evaluated in the order of their priority numbers. Maximum value for default syntax policies is 2147483647 and for classic policies is 64000. Minimum value = 0 Maximum value = 2147483647
bindpoint	<String>	Read-write	Bind point to which to bind the policy. Applies only to rewrite and cache policies. If you do not set this parameter, the policy is bound to REQ_DEFAULT or RES_DEFAULT, depending on whether the policy rule is a response-

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			time or a request-time expression. Possible values = REQUEST, RESPONSE, ICA_REQUEST, OTHERTCP_REQUEST, AAA_REQUEST, AAA_RESPONSE
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/ vpnvserver_authenticationloginschemapolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"vpnvserver_authenticationloginschemapolicy_binding":{

<b>"name":<String_value>,

</b>"policy":<String_value>,

"priority":<Integer_value>,

"secondary":<Boolean_value>,

"groupextraction":<Boolean_value>,

"gotopriorityexpression":<String_value>,

"bindpoint":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_authenticationloginschemapolicy_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_authenticationloginschemapolicy_binding/ name_value<String> ? **args=policy: <String_value> ,secondary: <Boolean_value> ,groupextraction: <Boolean_value> ,bindpoint: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_authenticationloginschemapolicy_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_authenticationloginschemapolicy_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of vpnvserver_authenticationloginschemapolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_authenticationloginschemapolicy_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vpnvserver_authenticationloginschemapolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnvserver_authenticationloginschemapolicy_binding": [ {

"gotopriorityexpression":<String_value>,

"policy":<String_value>,

"groupextraction":<Boolean_value>,

"name":<String_value>,

"secondary":<Boolean_value>,

"priority":<Integer_value>,

"bindpoint":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_authenticationloginschemapolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_authenticationloginschemapolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnvserver_authenticationloginschemapolicy_binding": [ {

"gotopriorityexpression":<String_value>,

"policy":<String_value>,

"groupextraction":<Boolean_value>,

"name":<String_value>,

"secondary":<Boolean_value>,

"priority":<Integer_value>,

"bindpoint":<String_value>
```

```
}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_authenticationloginschemapolicy_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"vpnvserver_authenticationloginschemapolicy_binding": [ { "__count":
"#no"} ] }
```

vpnvserver_authenticationnegotiatepolicy_binding

Binding object showing the authenticationnegotiatepolicy that can be bound to vpnvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
priority	<Integer>	Read-write	Integer specifying the policy's priority. The lower the number, the higher

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			the priority. Policies are evaluated in the order of their priority numbers. Maximum value for default syntax policies is 2147483647 and for classic policies is 64000. Minimum value = 0 Maximum value = 2147483647
bindpoint	<String>	Read-write	Bind point to which to bind the policy. Applies only to rewrite and cache policies. If you do not set this parameter, the policy is bound to REQ_DEFAULT or RES_DEFAULT, depending on whether the policy rule is a response-time or a request-time expression. Possible values = REQUEST, RESPONSE, ICA_REQUEST, OTHERTCP_REQUEST, AAA_REQUEST, AAA_RESPONSE
secondary	<Boolean>	Read-write	Binds the authentication policy as the secondary

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			policy to use in a two-factor configuration. A user must then authenticate not only via a primary authentication method but also via a secondary authentication method. User groups are aggregated across both. The user name must be exactly the same for both authentication methods, but they can require different passwords.
name	<String>	Read-write	Name of the virtual server. Minimum length = 1
policy	<String>	Read-write	The name of the policy, if any, bound to the VPN virtual server.
gotopriorityexpression	<String>	Read-write	Applicable only to advance vpn session policy. Expression or other value specifying the next policy to evaluate if the current policy evaluates to TRUE. Specify one of the following values: * NEXT - Evaluate the policy with the next

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			higher priority number. * END - End policy evaluation. * An expression that evaluates to a number. If you specify an expression, the number to which it evaluates determines the next policy to evaluate, as follows: * If the expression evaluates to a higher numbered priority, the policy with that priority is evaluated next. * If the expression evaluates to the priority of the current policy, the policy with the next higher numbered priority is evaluated next. * If the expression evaluates to a number that is larger than the largest numbered priority, policy evaluation ends. An UNDEF event is triggered if: * The expression is invalid. * The expression evaluates to a priority number that is numerically lower than the current policy's priority. * The

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			expression evaluates to a priority number that is between the current policy's priority number (say, 30) and the highest priority number (say, 100), but does not match any configured priority number (for example, the expression evaluates to the number 85). This example assumes that the priority number increments by 10 for every successive policy, and therefore a priority number of 85 does not exist in the policy label.
groupextraction	<Boolean>	Read-write	Binds the authentication policy to a tertiary chain which will be used only for group extraction. The user will not authenticate against this server, and this will only be called if primary and/or secondary authentication has succeeded.
acttype	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/vpnvserver_authenticationnegotiatepolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"vpnvserver_authenticationnegotiatepolicy_binding":{

<b>"name":<String_value>,

</b>"policy":<String_value>,

"priority":<Integer_value>,

"secondary":<Boolean_value>,

"groupextraction":<Boolean_value>,

"gotopriorityexpression":<String_value>,

"bindpoint":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_authenticationnegotiatepolicy_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_authenticationnegotiatepolicy_binding/ name_value<String> ? **args=policy: <String_value> ,secondary: <Boolean_value> ,groupextraction: <Boolean_value> ,bindpoint: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_authenticationnegotiatepolicy_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_authenticationnegotiatepolicy_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of vpnvserver_authenticationnegotiatepolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_authenticationnegotiatepolicy_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vpnvserver_authenticationnegotiatepolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnvserver_authenticationnegotiatepolicy_binding": [ {

"priority":<Integer_value>,

"bindpoint":<String_value>,

"secondary":<Boolean_value>,

"name":<String_value>,

"policy":<String_value>,

"gotopriorityexpression":<String_value>,

"groupextraction":<Boolean_value>,

"acttype":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_authenticationnegotiatepolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_authenticationnegotiatepolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnvserver_authenticationnegotiatepolicy_binding": [ {

"priority":<Integer_value>,

"bindpoint":<String_value>,

"secondary":<Boolean_value>,

"name":<String_value>,

"policy":<String_value>,

"gotopriorityexpression":<String_value>,

"groupextraction":<Boolean_value>,

"acttype":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_authenticationnegotiatepolicy_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"vpnvserver_authenticationnegotiatepolicy_binding": [ { "__count":
"#no"} ] }
```

vpnvserver_authenticationoauthidppolicy_binding

Binding object showing the authenticationoauthidppolicy that can be bound to vpnvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
groupextraction	<Boolean>	Read-write	Binds the authentication policy to a tertiary chain which will be used only for group extraction. The user will not authenticate against this server, and this will only be called if primary and/or secondary authentication has succeeded.
policy	<String>	Read-write	The name of the policy, if any, bound to the VPN virtual server.
gotopriorityexpression	<String>	Read-write	Next priority expression.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
priority	<Integer>	Read-write	Integer specifying the policy's priority. The lower the number, the higher the priority. Policies are evaluated in the order of their priority numbers. Maximum value for default syntax policies is 2147483647 and for classic policies is 64000. Minimum value = 0 Maximum value = 2147483647
bindpoint	<String>	Read-write	Bind point to which to bind the policy. Applies only to rewrite and cache policies. If you do not set this parameter, the policy is bound to REQ_DEFAULT or RES_DEFAULT, depending on whether the policy rule is a response-time or a request-time expression. Possible values = REQUEST, RESPONSE, ICA_REQUEST, OTHERTCP_REQUEST,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			AAA_REQUEST, AAA_RESPONSE
secondary	<Boolean>	Read-write	Binds the authentication policy as the secondary policy to use in a two-factor configuration. A user must then authenticate not only via a primary authentication method but also via a secondary authentication method. User groups are aggregated across both. The user name must be exactly the same for both authentication methods, but they can require different passwords.
name	<String>	Read-write	Name of the virtual server. Minimum length = 1
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)

- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/vpnvserver_authenticationoauthidppolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"vpnvserver_authenticationoauthidppolicy_binding":{

<b>"name":<String_value>,

</b>"policy":<String_value>,

"priority":<Integer_value>,

"secondary":<Boolean_value>,

"groupextraction":<Boolean_value>,

"gotopriorityexpression":<String_value>,

"bindpoint":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_authenticationoauthidppolicy_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_authenticationoauthidppolicy_binding/ name_value<String> ? **args=policy: <String_value> ,secondary: <Boolean_value> ,groupextraction: <Boolean_value> ,bindpoint: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_authenticationoauthidppolicy_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_authenticationoauthidppolicy_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of vpnvserver_authenticationoauthidppolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_authenticationoauthidppolicy_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vpnvserver_authenticationoauthidppolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnvserver_authenticationoauthidppolicy_binding": [ {

"groupextraction":<Boolean_value>,

"policy":<String_value>,
```

```
"gotopriorityexpression":<String_value>,

"priority":<Integer_value>,

"bindpoint":<String_value>,

"secondary":<Boolean_value>,

"name":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_authenticationoauthidppolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_authenticationoauthidppolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnvserver_authenticationoauthidppolicy_binding": [ {

"groupextraction":<Boolean_value>,

"policy":<String_value>,

"gotopriorityexpression":<String_value>,

"priority":<Integer_value>,

"bindpoint":<String_value>,

"secondary":<Boolean_value>,

"name":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_authenticationoauthidppolicy_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"vpnvserver_authenticationoauthidppolicy_binding": [ { "__count":
"#no"} ] }
```

vpnvserver_authenticationpolicy_binding

Binding object showing the authenticationpolicy that can be bound to vpnvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
priority	<Integer>	Read-write	Integer specifying the policy's priority. The lower the number, the higher the priority. Policies are evaluated in the order of their priority numbers. Maximum value for default syntax policies is 2147483647 and for classic policies is 64000. Minimum value = 0 Maximum value = 2147483647
bindpoint	<String>	Read-write	Bind point to which to bind the policy. Applies only to rewrite and cache policies. If you do not set this parameter, the policy is bound to REQ_DEFAULT or RES_DEFAULT, depending on whether the policy

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			rule is a response-time or a request-time expression. Possible values = REQUEST, RESPONSE, ICA_REQUEST, OTHERTCP_REQUEST, AAA_REQUEST, AAA_RESPONSE
name	<String>	Read-write	Name of the virtual server. Minimum length = 1
secondary	<Boolean>	Read-write	Binds the authentication policy as the secondary policy to use in a two-factor configuration. A user must then authenticate not only via a primary authentication method but also via a secondary authentication method. User groups are aggregated across both. The user name must be exactly the same for both authentication methods, but they can require different passwords.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
gotopriorityexpression	<String>	Read-write	Applicable only to advance vpn session policy. Expression or other value specifying the next policy to evaluate if the current policy evaluates to TRUE. Specify one of the following values: * NEXT - Evaluate the policy with the next higher priority number. * END - End policy evaluation. * An expression that evaluates to a number. If you specify an expression, the number to which it evaluates determines the next policy to evaluate, as follows: * If the expression evaluates to a higher numbered priority, the policy with that priority is evaluated next. * If the expression evaluates to the priority of the current policy, the policy with the next higher numbered priority is evaluated next. * If the expression evaluates to a number that is larger than the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			largest numbered priority, policy evaluation ends. An UNDEF event is triggered if: * The expression is invalid. * The expression evaluates to a priority number that is numerically lower than the current policy's priority. * The expression evaluates to a priority number that is between the current policy's priority number (say, 30) and the highest priority number (say, 100), but does not match any configured priority number (for example, the expression evaluates to the number 85). This example assumes that the priority number increments by 10 for every successive policy, and therefore a priority number of 85 does not exist in the policy label.
policy	<String>	Read-write	The name of the policy, if any, bound to the VPN virtual server.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
groupextraction	<Boolean>	Read-write	Binds the authentication policy to a tertiary chain which will be used only for group extraction. The user will not authenticate against this server, and this will only be called if primary and/or secondary authentication has succeeded.
acttype	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/vpnvserver_authenticationpolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"vpnvserver_authenticationpolicy_binding":{

<b>"name":<String_value>,

</b>"policy":<String_value>,

"priority":<Integer_value>,

"secondary":<Boolean_value>,

"groupextraction":<Boolean_value>,
```

```
"gotopriorityexpression":<String_value>,

"bindpoint":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_authenticationpolicy_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_authenticationpolicy_binding/ name_value<String> ? **args=policy: <String_value> ,secondary: <Boolean_value> ,groupextraction: <Boolean_value> ,bindpoint: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_authenticationpolicy_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_authenticationpolicy_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of vpnvserver_authenticationpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_authenticationpolicy_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vpnvserver_authenticationpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnvserver_authenticationpolicy_binding": [ {

"priority":<Integer_value>,

"bindpoint":<String_value>,

"name":<String_value>,

"secondary":<Boolean_value>,

"gotopriorityexpression":<String_value>,

"policy":<String_value>,

"groupextraction":<Boolean_value>,

"acttype":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_authenticationpolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_authenticationpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnvserver_authenticationpolicy_binding": [ {

"priority":<Integer_value>,

"bindpoint":<String_value>,

"name":<String_value>,

"secondary":<Boolean_value>,

"gotopriorityexpression":<String_value>,

"policy":<String_value>,

"groupextraction":<Boolean_value>,
```

```
"acttype":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_authenticationpolicy_binding/name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"vpnvserver_authenticationpolicy_binding": [ { "__count": "#no"} ] }
```

vpnvserver_authenticationradiuspolicy_binding

Binding object showing the authenticationradiuspolicy that can be bound to vpnvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
policy	<String>	Read-write	The name of the policy, if any, bound to the VPN virtual server.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
gotopriorityexpression	<String>	Read-write	Applicable only to advance vpn session policy. Expression or other value specifying the next policy to evaluate if the current policy evaluates to TRUE. Specify one of the following values: * NEXT - Evaluate the policy with the next higher priority number. * END - End policy evaluation. * An expression that evaluates to a number. If you specify an expression, the number to which it evaluates determines the next policy to evaluate, as follows: * If the expression evaluates to a higher numbered priority, the policy with that priority is evaluated next. * If the expression evaluates to the priority of the current policy, the policy with the next higher numbered priority is evaluated next. * If the expression evaluates to a number that is larger than the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			largest numbered priority, policy evaluation ends. An UNDEF event is triggered if: * The expression is invalid. * The expression evaluates to a priority number that is numerically lower than the current policy's priority. * The expression evaluates to a priority number that is between the current policy's priority number (say, 30) and the highest priority number (say, 100), but does not match any configured priority number (for example, the expression evaluates to the number 85). This example assumes that the priority number increments by 10 for every successive policy, and therefore a priority number of 85 does not exist in the policy label.
groupextraction	<Boolean>	Read-write	Binds the authentication policy to a tertiary chain which will be used only for group

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			extraction. The user will not authenticate against this server, and this will only be called if primary and/or secondary authentication has succeeded.
secondary	<Boolean>	Read-write	Binds the authentication policy as the secondary policy to use in a two-factor configuration. A user must then authenticate not only via a primary authentication method but also via a secondary authentication method. User groups are aggregated across both. The user name must be exactly the same for both authentication methods, but they can require different passwords.
name	<String>	Read-write	Name of the virtual server. Minimum length = 1
priority	<Integer>	Read-write	Integer specifying the policy's priority. The lower the number, the higher the priority. Policies

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			are evaluated in the order of their priority numbers. Maximum value for default syntax policies is 2147483647 and for classic policies is 64000. Minimum value = 0 Maximum value = 2147483647
bindpoint	<String>	Read-write	Bind point to which to bind the policy. Applies only to rewrite and cache policies. If you do not set this parameter, the policy is bound to REQ_DEFAULT or RES_DEFAULT, depending on whether the policy rule is a response-time or a request-time expression. Possible values = REQUEST, RESPONSE, ICA_REQUEST, OTHERTCP_REQUEST, AAA_REQUEST, AAA_RESPONSE
acttype	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/vpnvserver_authenticationradiuspolicy_binding
HTTP Method: PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"vpnvserver_authenticationradiuspolicy_binding":{

<b>"name":<String_value>,

</b>"policy":<String_value>,

"priority":<Integer_value>,

"secondary":<Boolean_value>,

"groupextraction":<Boolean_value>,

"gotopriorityexpression":<String_value>,

"bindpoint":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_authenticationradiuspolicy_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_authenticationradiuspolicy_binding/ name_value<String> ? **args=policy: <String_value> ,secondary: <Boolean_value> ,groupextraction: <Boolean_value> ,bindpoint: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_authenticationradiuspolicy_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_authenticationradiuspolicy_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of vpnvserver_authenticationradiuspolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_authenticationradiuspolicy_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vpnvserver_authenticationradiuspolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnvserver_authenticationradiuspolicy_binding": [ {

"policy":<String_value>,

"gotopriorityexpression":<String_value>,

"groupextraction":<Boolean_value>,

"secondary":<Boolean_value>,

"name":<String_value>,

"priority":<Integer_value>,

"bindpoint":<String_value>,

"acttype":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_authenticationradiuspolicy_binding
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_authenticationradiuspolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnvserver_authenticationradiuspolicy_binding": [ {

"policy":<String_value>,

"gotopriorityexpression":<String_value>,

"groupextraction":<Boolean_value>,

"secondary":<Boolean_value>,

"name":<String_value>,

"priority":<Integer_value>,

"bindpoint":<String_value>,

"acttype":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_authenticationradiuspolicy_binding/name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"vpnvserver_authenticationradiuspolicy_binding": [ { "__count":
"#no"} ] }
```

vpnvserver_authenticationsamlidppolicy_binding

Binding object showing the authenticationsamlidppolicy that can be bound to vpnvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
priority	<Integer>	Read-write	Integer specifying the policy's priority. The lower the number, the higher the priority. Policies are evaluated in the order of their priority numbers. Maximum value for default syntax policies is 2147483647 and for classic policies is 64000. Minimum value = 0 Maximum value = 2147483647
bindpoint	<String>	Read-write	Bind point to which to bind the policy. Applies only to rewrite and cache policies. If you do not set this parameter, the policy is bound to

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			REQ_DEFAULT or RES_DEFAULT, depending on whether the policy rule is a response-time or a request-time expression. Possible values = REQUEST, RESPONSE, ICA_REQUEST, OTHERTCP_REQUEST, AAA_REQUEST, AAA_RESPONSE
name	<String>	Read-write	Name of the virtual server. Minimum length = 1
secondary	<Boolean>	Read-write	Binds the authentication policy as the secondary policy to use in a two-factor configuration. A user must then authenticate not only via a primary authentication method but also via a secondary authentication method. User groups are aggregated across both. The user name must be exactly the same for both authentication methods, but they

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			can require different passwords.
gotopriorityexpression	<String>	Read-write	Next priority expression.
policy	<String>	Read-write	The name of the policy, if any, bound to the VPN virtual server.
groupextraction	<Boolean>	Read-write	Binds the authentication policy to a tertiary chain which will be used only for group extraction. The user will not authenticate against this server, and this will only be called if primary and/or secondary authentication has succeeded.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/vpnvserver_authenticationsamlidppolicy_binding
HTTP Method: PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"vpnvserver_authenticationsamlidppolicy_binding":{

<b>"name":<String_value>,
```

```
</b>"policy":<String_value>,

"priority":<Integer_value>,

"secondary":<Boolean_value>,

"groupextraction":<Boolean_value>,

"gotopriorityexpression":<String_value>,

"bindpoint":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_authenticationsamlidppolicy_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_authenticationsamlidppolicy_binding/ name_value<String> ? **args=policy: <String_value> ,secondary: <Boolean_value> ,groupextraction: <Boolean_value> ,bindpoint: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_authenticationsamlidppolicy_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_authenticationsamlidppolicy_binding/

name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of vpnvserver_authenticationsamlidppolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_authenticationsamlidppolicy_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vpnvserver_authenticationsamlidppolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnvserver_authenticationsamlidppolicy_binding": [ {

"priority":<Integer_value>,

"bindpoint":<String_value>,

"name":<String_value>,

"secondary":<Boolean_value>,

"gotopriorityexpression":<String_value>,
```

```
"policy":<String_value>,

"groupextraction":<Boolean_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_authenticationsamlidppolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_authenticationsamlidppolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnvserver_authenticationsamlidppolicy_binding": [ {

"priority":<Integer_value>,

"bindpoint":<String_value>,

"name":<String_value>,
```

```
"secondary":<Boolean_value>,

"gotopriorityexpression":<String_value>,

"policy":<String_value>,

"groupextraction":<Boolean_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_authenticationsamlidppolicy_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"vpnvserver_authenticationsamlidppolicy_binding": [ { "__count":
"#no"} ] }
```

vpnvserver_authenticationsamlpolicy_binding

Binding object showing the authenticationsamlpolicy that can be bound to vpnvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
secondary	<Boolean>	Read-write	Binds the authentication policy as the secondary policy to use in a two-factor configuration. A user must then authenticate not only via a primary authentication method but also via a secondary authentication method. User groups are aggregated across both. The user name must be exactly the same for both authentication methods, but they can require different passwords.
name	<String>	Read-write	Name of the virtual server. Minimum length = 1
priority	<Integer>	Read-write	Integer specifying the policy's priority. The lower the number, the higher the priority. Policies are evaluated in the order of their priority numbers. Maximum value for default syntax policies is 2147483647 and for

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			classic policies is 64000. Minimum value = 0 Maximum value = 2147483647
bindpoint	<String>	Read-write	Bind point to which to bind the policy. Applies only to rewrite and cache policies. If you do not set this parameter, the policy is bound to REQ_DEFAULT or RES_DEFAULT, depending on whether the policy rule is a response-time or a request-time expression. Possible values = REQUEST, RESPONSE, ICA_REQUEST, OTHERTCP_REQUEST, AAA_REQUEST, AAA_RESPONSE
groupextraction	<Boolean>	Read-write	Binds the authentication policy to a tertiary chain which will be used only for group extraction. The user will not authenticate against this server, and this will only be called if primary and/

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			or secondary authentication has succeeded.
policy	<String>	Read-write	The name of the policy, if any, bound to the VPN virtual server.
gotopriorityexpression	<String>	Read-write	Applicable only to advance vpn session policy. Expression or other value specifying the next policy to evaluate if the current policy evaluates to TRUE. Specify one of the following values: * NEXT - Evaluate the policy with the next higher priority number. * END - End policy evaluation. * An expression that evaluates to a number. If you specify an expression, the number to which it evaluates determines the next policy to evaluate, as follows: * If the expression evaluates to a higher numbered priority, the policy with that priority is evaluated next. * If the expression evaluates

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			to the priority of the current policy, the policy with the next higher numbered priority is evaluated next. * If the expression evaluates to a number that is larger than the largest numbered priority, policy evaluation ends. An UNDEF event is triggered if: * The expression is invalid. * The expression evaluates to a priority number that is numerically lower than the current policy's priority. * The expression evaluates to a priority number that is between the current policy's priority number (say, 30) and the highest priority number (say, 100), but does not match any configured priority number (for example, the expression evaluates to the number 85). This example assumes that the priority number increments by 10 for every successive policy, and therefore

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			a priority number of 85 does not exist in the policy label.
acttype	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/vpnvserver_authenticationsamlpolicy_binding
HTTP Method: PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"vpnvserver_authenticationsamlpolicy_binding":{

<b>"name":<String_value>,

</b>"policy":<String_value>,

"priority":<Integer_value>,

"secondary":<Boolean_value>,

"groupextraction":<Boolean_value>,

"gotopriorityexpression":<String_value>,

"bindpoint":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_authenticationsamlpolicy_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_authenticationsamlpolicy_binding/ name_value<String> ? **args=policy: <String_value> ,secondary: <Boolean_value> ,groupextraction: <Boolean_value> ,bindpoint: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_authenticationsamlpolicy_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_authenticationsamlpolicy_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of vpnvserver_authenticationsamlpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_authenticationsamlpolicy_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vpnvserver_authenticationsamlpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnvserver_authenticationsamlpolicy_binding": [ {

"secondary":<Boolean_value>,

"name":<String_value>,

"priority":<Integer_value>,

"bindpoint":<String_value>,

"groupextraction":<Boolean_value>,

"policy":<String_value>,

"gotopriorityexpression":<String_value>,

"acttype":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_authenticationsamlpolicy_binding
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_authenticationsamlpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnvserver_authenticationsamlpolicy_binding": [ {

"secondary":<Boolean_value>,

"name":<String_value>,

"priority":<Integer_value>,

"bindpoint":<String_value>,

"groupextraction":<Boolean_value>,

"policy":<String_value>,

"gotopriorityexpression":<String_value>,

"acttype":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_authenticationsamlpolicy_binding/name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"vpnvserver_authenticationsamlpolicy_binding": [ { "__count": "#no"} ] }
```

vpnvserver_authenticationtacacspolicy_binding

Binding object showing the authenticationtacacspolicy that can be bound to vpnvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
secondary	<Boolean>	Read-write	Binds the authentication policy as the secondary policy to use in a two-factor configuration. A user must then authenticate not only via a primary authentication method but also via a secondary authentication method. User groups are aggregated across both. The user name must be exactly the same for

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			both authentication methods, but they can require different passwords.
name	<String>	Read-write	Name of the virtual server. Minimum length = 1
bindpoint	<String>	Read-write	Bind point to which to bind the policy. Applies only to rewrite and cache policies. If you do not set this parameter, the policy is bound to REQ_DEFAULT or RES_DEFAULT, depending on whether the policy rule is a response-time or a request-time expression. Possible values = REQUEST, RESPONSE, ICA_REQUEST, OTHERTCP_REQUEST, AAA_REQUEST, AAA_RESPONSE
priority	<Integer>	Read-write	Integer specifying the policy's priority. The lower the number, the higher the priority. Policies are evaluated in the order of their priority numbers. Maximum

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			value for default syntax policies is 2147483647 and for classic policies is 64000. Minimum value = 0 Maximum value = 2147483647
policy	<String>	Read-write	The name of the policy, if any, bound to the VPN virtual server.
gotopriorityexpression	<String>	Read-write	Applicable only to advance vpn session policy. Expression or other value specifying the next policy to evaluate if the current policy evaluates to TRUE. Specify one of the following values: * NEXT - Evaluate the policy with the next higher priority number. * END - End policy evaluation. * An expression that evaluates to a number. If you specify an expression, the number to which it evaluates determines the next policy to evaluate, as follows: * If the expression evaluates

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			to a higher numbered priority, the policy with that priority is evaluated next. * If the expression evaluates to the priority of the current policy, the policy with the next higher numbered priority is evaluated next. * If the expression evaluates to a number that is larger than the largest numbered priority, policy evaluation ends. An UNDEF event is triggered if: * The expression is invalid. * The expression evaluates to a priority number that is numerically lower than the current policy's priority. * The expression evaluates to a priority number that is between the current policy's priority number (say, 30) and the highest priority number (say, 100), but does not match any configured priority number (for example, the expression evaluates to the number 85).

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			This example assumes that the priority number increments by 10 for every successive policy, and therefore a priority number of 85 does not exist in the policy label.
groupextraction	<Boolean>	Read-write	Binds the authentication policy to a tertiary chain which will be used only for group extraction. The user will not authenticate against this server, and this will only be called if primary and/or secondary authentication has succeeded.
acttype	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/vpnvserver_authenticationtacacspolicy_binding
HTTP Method: PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"vpnvserver_authenticationtacacspolicy_binding":{

<b>"name":<String_value>,
```

```
</b>"policy":<String_value>,

"priority":<Integer_value>,

"secondary":<Boolean_value>,

"groupextraction":<Boolean_value>,

"gotopriorityexpression":<String_value>,

"bindpoint":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_authenticationtacacspolicy_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_authenticationtacacspolicy_binding/ name_value<String> ? **args=policy: <String_value> ,secondary: <Boolean_value> ,groupextraction: <Boolean_value> ,bindpoint: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_authenticationtacacspolicy_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_authenticationtacacspolicy_binding/

name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of vpnvserver_authenticationtacacspolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_authenticationtacacspolicy_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vpnvserver_authenticationtacacspolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnvserver_authenticationtacacspolicy_binding": [ {

"secondary":<Boolean_value>,

"name":<String_value>,

"bindpoint":<String_value>,

"priority":<Integer_value>,

"policy":<String_value>,
```

```
"gotopriorityexpression":<String_value>,

"groupextraction":<Boolean_value>,

"acttype":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_authenticationtacacspolicy_binding
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_authenticationtacacspolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnvserver_authenticationtacacspolicy_binding": [ {

"secondary":<Boolean_value>,

"name":<String_value>,
```

```
"bindpoint":<String_value>,

"priority":<Integer_value>,

"policy":<String_value>,

"gotopriorityexpression":<String_value>,

"groupextraction":<Boolean_value>,

"acttype":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_authenticationtacacspolicy_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"vpnvserver_authenticationtacacspolicy_binding": [ { "__count":
"#no"} ] }
```

vpnvserver_authenticationwebauthpolicy_binding

Binding object showing the authenticationwebauthpolicy that can be bound to vpnvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the virtual server. Minimum length = 1
secondary	<Boolean>	Read-write	Binds the authentication policy as the secondary policy to use in a two-factor configuration. A user must then authenticate not only via a primary authentication method but also via a secondary authentication method. User groups are aggregated across both. The user name must be exactly the same for both authentication methods, but they can require different passwords.
bindpoint	<String>	Read-write	Bind point to which to bind the policy. Applies only to rewrite and cache policies. If you do not set this parameter, the policy is bound to

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			REQ_DEFAULT or RES_DEFAULT, depending on whether the policy rule is a response-time or a request-time expression. Possible values = REQUEST, RESPONSE, ICA_REQUEST, OTHERTCP_REQUEST, AAA_REQUEST, AAA_RESPONSE
priority	<Integer>	Read-write	Integer specifying the policy's priority. The lower the number, the higher the priority. Policies are evaluated in the order of their priority numbers. Maximum value for default syntax policies is 2147483647 and for classic policies is 64000. Minimum value = 0 Maximum value = 2147483647
gotopriorityexpression	<String>	Read-write	Applicable only to advance vpn session policy. Expression or other value specifying the next policy to evaluate if

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			the current policy evaluates to TRUE. Specify one of the following values: * NEXT - Evaluate the policy with the next higher priority number. * END - End policy evaluation. * An expression that evaluates to a number. If you specify an expression, the number to which it evaluates determines the next policy to evaluate, as follows: * If the expression evaluates to a higher numbered priority, the policy with that priority is evaluated next. * If the expression evaluates to the priority of the current policy, the policy with the next higher numbered priority is evaluated next. * If the expression evaluates to a number that is larger than the largest numbered priority, policy evaluation ends. An UNDEF event is triggered if: * The expression is invalid.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			* The expression evaluates to a priority number that is numerically lower than the current policy's priority. * The expression evaluates to a priority number that is between the current policy's priority number (say, 30) and the highest priority number (say, 100), but does not match any configured priority number (for example, the expression evaluates to the number 85). This example assumes that the priority number increments by 10 for every successive policy, and therefore a priority number of 85 does not exist in the policy label.
policy	<String>	Read-write	The name of the policy, if any, bound to the VPN virtual server.
groupextraction	<Boolean>	Read-write	Binds the authentication policy to a tertiary chain which will be used only for group extraction. The user

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			will not authenticate against this server, and this will only be called if primary and/or secondary authentication has succeeded.
acttype	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/ vpnvserver_authenticationwebauthpolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"vpnvserver_authenticationwebauthpolicy_binding":{

<b>"name":<String_value>,

</b>"policy":<String_value>,

"priority":<Integer_value>,

"secondary":<Boolean_value>,

"groupextraction":<Boolean_value>,

"gotopriorityexpression":<String_value>,

"bindpoint":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_authenticationwebauthpolicy_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_authenticationwebauthpolicy_binding/ name_value<String> ? **args=policy: <String_value> ,secondary: <Boolean_value> ,groupextraction: <Boolean_value> ,bindpoint: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_authenticationwebauthpolicy_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_authenticationwebauthpolicy_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of vpnvserver_authenticationwebauthpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_authenticationwebauthpolicy_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vpnvserver_authenticationwebauthpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnvserver_authenticationwebauthpolicy_binding": [ {

"name":<String_value>,

"secondary":<Boolean_value>,

"bindpoint":<String_value>,

"priority":<Integer_value>,

"gotopriorityexpression":<String_value>,

"policy":<String_value>,

"groupextraction":<Boolean_value>,

"acttype":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_authenticationwebauthpolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_authenticationwebauthpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnvserver_authenticationwebauthpolicy_binding": [ {

"name":<String_value>,

"secondary":<Boolean_value>,

"bindpoint":<String_value>,

"priority":<Integer_value>,

"gotopriorityexpression":<String_value>,

"policy":<String_value>,

"groupextraction":<Boolean_value>,

"acttype":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_authenticationwebauthpolicy_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"vpnvserver_authenticationwebauthpolicy_binding": [ { "__count":
"#no"} ] }
```

vpnvserver_binding

Binding object which returns the resources bound to vpnvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the Citrix Gateway virtual server for which to show detailed information. Minimum length = 1
vpnvserver_cspolicy_binding	<vpnvserver_cspolicy_binding[]>	Read-only	cspolicy that can be bound to vpnvserver.
vpnvserver_vpnurlpolicy_binding	<vpnvserver_vpnurlpolicy_binding[]>	Read-only	vpnurlpolicy that can be bound to vpnvserver.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
vpnvserver_vpnurl_binding	<vpnvserver_vpnurl_binding[]>	Read-only	vpnurl that can be bound to vpnvserver.
vpnvserver_authenticationnegotiatepolicy_binding	<vpnvserver_authenticationnegotiatepolicy_binding[]>	Read-only	authenticationnegotiatepolicy that can be bound to vpnvserver.
vpnvserver_appfwpolicy_binding	<vpnvserver_appfwpolicy_binding[]>	Read-only	appfwpolicy that can be bound to vpnvserver.
vpnvserver_authenticationdfapolicy_binding	<vpnvserver_authenticationdfapolicy_binding[]>	Read-only	authenticationdfapolicy that can be bound to vpnvserver.
vpnvserver_auditsyslogpolicy_binding	<vpnvserver_auditsyslogpolicy_binding[]>	Read-only	auditsyslogpolicy that can be bound to vpnvserver.
vpnvserver_vpnsecureprivateaccessprofile_binding	<vpnvserver_vpnsecureprivateaccessprofile_binding[]>	Read-only	vpnsecureprivateaccessprofile that can be bound to vpnvserver.
vpnvserver_vpnsessionpolicy_binding	<vpnvserver_vpnsessionpolicy_binding[]>	Read-only	vpnsessionpolicy that can be bound to vpnvserver.
vpnvserver_authenticationsamlidppolicy_binding	<vpnvserver_authenticationsamlidppolicy_binding[]>	Read-only	authenticationsamlidppolicy that can be bound to vpnvserver.
vpnvserver_rewritepolicy_binding	<vpnvserver_rewritepolicy_binding[]>	Read-only	rewritepolicy that can be bound to vpnvserver.
vpnvserver_vpnepaprofile_binding	<vpnvserver_vpnepaprofile_binding[]>	Read-only	vpnepaprofile that can be bound to vpnvserver.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
vpnvserver_feopolicy_binding	<vpnvserver_feopolicy_binding[]>	Read-only	feopolicy that can be bound to vpnvserver.
vpnvserver_vpnnexthopserver_binding	<vpnvserver_vpnnexthopserver_binding[]>	Read-only	vpnnexthopserver that can be bound to vpnvserver.
vpnvserver_cachepolicy_binding	<vpnvserver_cachepolicy_binding[]>	Read-only	cachepolicy that can be bound to vpnvserver.
vpnvserver_authenticationloginschemapolicy_binding	<vpnvserver_authenticationloginschemapolicy_binding[]>	Read-only	authenticationloginschemapolicy that can be bound to vpnvserver.
vpnvserver_authenticationlocalpolicy_binding	<vpnvserver_authenticationlocalpolicy_binding[]>	Read-only	authenticationlocalpolicy that can be bound to vpnvserver.
vpnvserver_authenticationwebauthpolicy_binding	<vpnvserver_authenticationwebauthpolicy_binding[]>	Read-only	authenticationwebauthpolicy that can be bound to vpnvserver.
vpnvserver_secureprivateaccessurl_binding	<vpnvserver_secureprivateaccessurl_binding[]>	Read-only	secureprivateaccessurl that can be bound to vpnvserver.
vpnvserver_vpnintranetapplication_binding	<vpnvserver_vpnintranetapplication_binding[]>	Read-only	vpnintranetapplication that can be bound to vpnvserver.
vpnvserver_intranetip6_binding	<vpnvserver_intranetip6_binding[]>	Read-only	intranetip6 that can be bound to vpnvserver.
vpnvserver_authenticationldappolicy_binding	<vpnvserver_authenticationldappolicy_binding[]>	Read-only	authenticationldappolicy that can be bound to vpnvserver.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
vpnvserver_vpneula_binding	<vpnvserver_vpneula_binding[]>	Read-only	vpneula that can be bound to vpnvserver.
vpnvserver_vpntrafficpolicy_binding	<vpnvserver_vpntrafficpolicy_binding[]>	Read-only	vpntrafficpolicy that can be bound to vpnvserver.
vpnvserver_authenticationradiuspolicy_binding	<vpnvserver_authenticationradiuspolicy_binding[]>	Read-only	authenticationradiuspolicy that can be bound to vpnvserver.
vpnvserver_appcontroller_binding	<vpnvserver_appcontroller_binding[]>	Read-only	appcontroller that can be bound to vpnvserver.
vpnvserver_analyticsprofile_binding	<vpnvserver_analyticsprofile_binding[]>	Read-only	analyticsprofile that can be bound to vpnvserver.
vpnvserver_vpnclientlessaccesspolicy_binding	<vpnvserver_vpnclientlessaccesspolicy_binding[]>	Read-only	vpnclientlessaccesspolicy that can be bound to vpnvserver.
vpnvserver_authenticationtacacspolicy_binding	<vpnvserver_authenticationtacacspolicy_binding[]>	Read-only	authenticationtacacspolicy that can be bound to vpnvserver.
vpnvserver_authenticationoauthidppolicy_binding	<vpnvserver_authenticationoauthidppolicy_binding[]>	Read-only	authenticationoauthidppolicy that can be bound to vpnvserver.
vpnvserver_appflowpolicy_binding	<vpnvserver_appflowpolicy_binding[]>	Read-only	appflowpolicy that can be bound to vpnvserver.
vpnvserver_vpnportaltheme_binding	<vpnvserver_vpnportaltheme_binding[]>	Read-only	vpnportaltheme that can be bound to vpnvserver.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
vpnvserver_authenticationcertpolicy_binding	<vpnvserver_authenticationcertpolicy_binding[]>	Read-only	authenticationcertpolicy that can be bound to vpnvserver.
vpnvserver_staserver_binding	<vpnvserver_staserver_binding[]>	Read-only	staserver that can be bound to vpnvserver.
vpnvserver_authenticationsamlpolicy_binding	<vpnvserver_authenticationsamlpolicy_binding[]>	Read-only	authenticationsamlpolicy that can be bound to vpnvserver.
vpnvserver_authenticationpolicy_binding	<vpnvserver_authenticationpolicy_binding[]>	Read-only	authenticationpolicy that can be bound to vpnvserver.
vpnvserver_aaapreauthenticationpolicy_binding	<vpnvserver_aaapreauthenticationpolicy_binding[]>	Read-only	aaapreauthenticationpolicy that can be bound to vpnvserver.
vpnvserver_sharefileserver_binding	<vpnvserver_sharefileserver_binding[]>	Read-only	sharefileserver that can be bound to vpnvserver.
vpnvserver_responderpolicy_binding	<vpnvserver_responderpolicy_binding[]>	Read-only	responderpolicy that can be bound to vpnvserver.
vpnvserver_intranetip_binding	<vpnvserver_intranetip_binding[]>	Read-only	intranetip that can be bound to vpnvserver.
vpnvserver_auditnslogpolicy_binding	<vpnvserver_auditnslogpolicy_binding[]>	Read-only	auditnslogpolicy that can be bound to vpnvserver.
vpnvserver_icapolicy_binding	<vpnvserver_icapolicy_binding[]>	Read-only	icapolicy that can be bound to vpnvserver.

Operations

(click to see Properties)

- GET

- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_binding/ name_value<String>
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vpnvserver_binding": [ {

"name":<String_value>,

"vpnvserver_authenticationwebauthpolicy_binding":<vpnvserver_authenticatio
nwebauthpolicy_binding[]_value>,

"vpnvserver_vpnsessionpolicy_binding":<vpnvserver_vpnsessionpolicy_binding
[]_value>,

"vpnvserver_authenticationldappolicy_binding":<vpnvserver_authenticationld
appolicy_binding[]_value>,

"vpnvserver_icapolicy_binding":<vpnvserver_icapolicy_binding[]_value>,

"vpnvserver_authenticationdfapolicy_binding":<vpnvserver_authenticationdfa
policy_binding[]_value>,

"vpnvserver_aaapreauthenticationpolicy_binding":<vpnvserver_aaapreauthenti
cationpolicy_binding[]_value>,

"vpnvserver_authenticationoauthidppolicy_binding":<vpnvserver_authenticati
onoauthidppolicy_binding[]_value>,

"vpnvserver_authenticationsamlpolicy_binding":<vpnvserver_authenticationsa
mlpolicy_binding[]_value>,

"vpnvserver_appcontroller_binding":<vpnvserver_appcontroller_binding[]_val
ue>,

"vpnvserver_authenticationradiuspolicy_binding":<vpnvserver_authentication
radiuspolicy_binding[]_value>,

"vpnvserver_rewritepolicy_binding":<vpnvserver_rewritepolicy_binding[]_val
ue>,

"vpnvserver_vpnepaprofile_binding":<vpnvserver_vpnepaprofile_binding[]_val
```

```
ue>,

"vpnvserver_authenticationcertpolicy_binding":<vpnvserver_authenticationcertpolicy_binding[]_value>,

"vpnvserver_appflowpolicy_binding":<vpnvserver_appflowpolicy_binding[]_value>,

"vpnvserver_auditnslogpolicy_binding":<vpnvserver_auditnslogpolicy_binding[]_value>,

"vpnvserver_authenticationlocalpolicy_binding":<vpnvserver_authenticationlocalpolicy_binding[]_value>,

"vpnvserver_vpnsecureprivateaccessprofile_binding":<vpnvserver_vpnsecureprivateaccessprofile_binding[]_value>,

"vpnvserver_authenticationpolicy_binding":<vpnvserver_authenticationpolicy_binding[]_value>,

"vpnvserver_feopolicy_binding":<vpnvserver_feopolicy_binding[]_value>,

"vpnvserver_secureprivateaccessurl_binding":<vpnvserver_secureprivateaccessurl_binding[]_value>,

"vpnvserver_vpneula_binding":<vpnvserver_vpneula_binding[]_value>,

"vpnvserver_responderpolicy_binding":<vpnvserver_responderpolicy_binding[]_value>,

"vpnvserver_authenticationsamlidppolicy_binding":<vpnvserver_authenticationsamlidppolicy_binding[]_value>,

"vpnvserver_vpnclientlessaccesspolicy_binding":<vpnvserver_vpnclientlessaccesspolicy_binding[]_value>,

"vpnvserver_staserver_binding":<vpnvserver_staserver_binding[]_value>,

"vpnvserver_intranetip_binding":<vpnvserver_intranetip_binding[]_value>,

"vpnvserver_vpnurlpolicy_binding":<vpnvserver_vpnurlpolicy_binding[]_value>,

"vpnvserver_cspolicy_binding":<vpnvserver_cspolicy_binding[]_value>,
```

```
"vpnvserver_sharefileserver_binding":<vpnvserver_sharefileserver_binding[]
_value>,

"vpnvserver_vpnurl_binding":<vpnvserver_vpnurl_binding[]_value>,

"vpnvserver_vpnnexthopserver_binding":<vpnvserver_vpnnexthopserver_binding
[]_value>,

"vpnvserver_vpnportaltheme_binding":<vpnvserver_vpnportaltheme_binding[]_v
alue>,

"vpnvserver_cachepolicy_binding":<vpnvserver_cachepolicy_binding[]_value>,

"vpnvserver_vpntrafficpolicy_binding":<vpnvserver_vpntrafficpolicy_binding
[]_value>,

"vpnvserver_intranetip6_binding":<vpnvserver_intranetip6_binding[]_value>,

"vpnvserver_auditsyslogpolicy_binding":<vpnvserver_auditsyslogpolicy_bindi
ng[]_value>,

"vpnvserver_appfwpolicy_binding":<vpnvserver_appfwpolicy_binding[]_value>,

"vpnvserver_authenticationloginschemapolicy_binding":<vpnvserver_authentic
ationloginschemapolicy_binding[]_value>,

"vpnvserver_authenticationnegotiatepolicy_binding":<vpnvserver_authenticat
ionnegotiatepolicy_binding[]_value>,

"vpnvserver_analyticsprofile_binding":<vpnvserver_analyticsprofile_binding
[]_value>,

"vpnvserver_vpnintranetapplication_binding":<vpnvserver_vpnintranetapplica
tion_binding[]_value>,

"vpnvserver_authenticationtacacspolicy_binding":<vpnvserver_authentication
tacacspolicy_binding[]_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "vpnvserver_binding": [ {

"name":<String_value>,

"vpnvserver_authenticationwebauthpolicy_binding":<vpnvserver_authenticatio
nwebauthpolicy_binding[]_value>,

"vpnvserver_vpnsessionpolicy_binding":<vpnvserver_vpnsessionpolicy_binding
[]_value>,

"vpnvserver_authenticationldappolicy_binding":<vpnvserver_authenticationld
appolicy_binding[]_value>,

"vpnvserver_icapolicy_binding":<vpnvserver_icapolicy_binding[]_value>,

"vpnvserver_authenticationdfapolicy_binding":<vpnvserver_authenticationdfa
policy_binding[]_value>,
```

```
"vpnvserver_aaapreauthenticationpolicy_binding":<vpnvserver_aaapreauthenti
cationpolicy_binding[]_value>,

"vpnvserver_authenticationoauthidppolicy_binding":<vpnvserver_authenticati
onoauthidppolicy_binding[]_value>,

"vpnvserver_authenticationsamlpolicy_binding":<vpnvserver_authenticationsa
mlpolicy_binding[]_value>,

"vpnvserver_appcontroller_binding":<vpnvserver_appcontroller_binding[]_val
ue>,

"vpnvserver_authenticationradiuspolicy_binding":<vpnvserver_authentication
radiuspolicy_binding[]_value>,

"vpnvserver_rewritepolicy_binding":<vpnvserver_rewritepolicy_binding[]_val
ue>,

"vpnvserver_vpnepaprofile_binding":<vpnvserver_vpnepaprofile_binding[]_val
ue>,

"vpnvserver_authenticationcertpolicy_binding":<vpnvserver_authenticationce
rtpolicy_binding[]_value>,

"vpnvserver_appflowpolicy_binding":<vpnvserver_appflowpolicy_binding[]_val
ue>,

"vpnvserver_auditnslogpolicy_binding":<vpnvserver_auditnslogpolicy_binding
[]_value>,

"vpnvserver_authenticationlocalpolicy_binding":<vpnvserver_authenticationl
ocalpolicy_binding[]_value>,

"vpnvserver_vpnsecureprivateaccessprofile_binding":<vpnvserver_vpnsecurepr
ivateaccessprofile_binding[]_value>,

"vpnvserver_authenticationpolicy_binding":<vpnvserver_authenticationpolicy
_binding[]_value>,

"vpnvserver_feopolicy_binding":<vpnvserver_feopolicy_binding[]_value>,

"vpnvserver_secureprivateaccessurl_binding":<vpnvserver_secureprivateacces
surl_binding[]_value>,
```

```
"vpnvserver_vpneula_binding":<vpnvserver_vpneula_binding[]_value>,

"vpnvserver_responderpolicy_binding":<vpnvserver_responderpolicy_binding[]
_value>,

"vpnvserver_authenticationsamlidppolicy_binding":<vpnvserver_authenticatio
nsamlidppolicy_binding[]_value>,

"vpnvserver_vpnclientlessaccesspolicy_binding":<vpnvserver_vpnclientlessac
cesspolicy_binding[]_value>,

"vpnvserver_staserver_binding":<vpnvserver_staserver_binding[]_value>,

"vpnvserver_intranetip_binding":<vpnvserver_intranetip_binding[]_value>,

"vpnvserver_vpnurlpolicy_binding":<vpnvserver_vpnurlpolicy_binding[]_value
>,

"vpnvserver_cspolicy_binding":<vpnvserver_cspolicy_binding[]_value>,

"vpnvserver_sharefileserver_binding":<vpnvserver_sharefileserver_binding[]
_value>,

"vpnvserver_vpnurl_binding":<vpnvserver_vpnurl_binding[]_value>,

"vpnvserver_vpnnexthopserver_binding":<vpnvserver_vpnnexthopserver_binding
[]_value>,

"vpnvserver_vpnportaltheme_binding":<vpnvserver_vpnportaltheme_binding[]_v
alue>,

"vpnvserver_cachepolicy_binding":<vpnvserver_cachepolicy_binding[]_value>,

"vpnvserver_vpntrafficpolicy_binding":<vpnvserver_vpntrafficpolicy_binding
[]_value>,

"vpnvserver_intranetip6_binding":<vpnvserver_intranetip6_binding[]_value>,

"vpnvserver_auditsyslogpolicy_binding":<vpnvserver_auditsyslogpolicy_bindi
ng[]_value>,

"vpnvserver_appfwpolicy_binding":<vpnvserver_appfwpolicy_binding[]_value>,
```

```
"vpnvserver_authenticationloginschemapolicy_binding":<vpnvserver_authentic
ationloginschemapolicy_binding[]_value>,

"vpnvserver_authenticationnegotiatepolicy_binding":<vpnvserver_authenticat
ionnegotiatepolicy_binding[]_value>,

"vpnvserver_analyticsprofile_binding":<vpnvserver_analyticsprofile_binding
[]_value>,

"vpnvserver_vpnintranetapplication_binding":<vpnvserver_vpnintranetapplica
tion_binding[]_value>,

"vpnvserver_authenticationtacacspolicy_binding":<vpnvserver_authentication
tacacspolicy_binding[]_value>

}]}
```

vpnvserver_cachepolicy_binding

Binding object showing the cachepolicy that can be bound to vpnvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
groupextraction	<Boolean>	Read-write	Binds the authentication policy to a tertiary chain which will be used only for group extraction. The user will not authenticate against this server, and this will only be called if primary and/or secondary authentication has succeeded.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
policy	<String>	Read-write	The name of the policy, if any, bound to the VPN virtual server.
gotopriorityexpression	<String>	Read-write	Next priority expression.
secondary	<Boolean>	Read-write	Binds the authentication policy as the secondary policy to use in a two-factor configuration. A user must then authenticate not only via a primary authentication method but also via a secondary authentication method. User groups are aggregated across both. The user name must be exactly the same for both authentication methods, but they can require different passwords.
name	<String>	Read-write	Name of the virtual server. Minimum length = 1
bindpoint	<String>	Read-write	Bindpoint to which the policy is bound. Possible values = REQUEST, RESPONSE,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			ICA_REQUEST, OTHERTCP_REQUEST, AAA_REQUEST, AAA_RESPONSE
priority	<Integer>	Read-write	Integer specifying the policy's priority. The lower the number, the higher the priority. Policies are evaluated in the order of their priority numbers. Maximum value for default syntax policies is 2147483647 and for classic policies is 64000. Minimum value = 0 Maximum value = 2147483647
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/vpnvserver_cachepolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"vpnvserver_cachepolicy_binding":{

<b>"name":<String_value>,
```

```
</b>"policy":<String_value>,

"priority":<Integer_value>,

"secondary":<Boolean_value>,

"groupextraction":<Boolean_value>,

"gotopriorityexpression":<String_value>,

"bindpoint":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_cachepolicy_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_cachepolicy_binding/ name_value<String> ? **args=policy: <String_value> ,secondary: <Boolean_value> ,groupextraction: <Boolean_value> ,bindpoint: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_cachepolicy_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/

vpnvserver_cachepolicy_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of vpnvserver_cachepolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_cachepolicy_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vpnvserver_cachepolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnvserver_cachepolicy_binding": [ {

"groupextraction":<Boolean_value>,

"policy":<String_value>,

"gotopriorityexpression":<String_value>,

"secondary":<Boolean_value>,

"name":<String_value>,

"bindpoint":<String_value>,
```

```
"priority":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_cachepolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_cachepolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnvserver_cachepolicy_binding": [ {

"groupextraction":<Boolean_value>,

"policy":<String_value>,

"gotopriorityexpression":<String_value>,

"secondary":<Boolean_value>,
```

```
"name":<String_value>,

"bindpoint":<String_value>,

"priority":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_cachepolicy_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"vpnvserver_cachepolicy_binding": [ { "__count": "#no"} ] }
```

vpnvserver_cspolicy_binding

Binding object showing the cspolicy that can be bound to vpnvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
bindpoint	<String>	Read-write	Bind point to which to bind the policy. Applies only to rewrite and cache policies. If you do not set this parameter, the policy is bound to REQ_DEFAULT or RES_DEFAULT, depending on whether the policy rule is a response-time or a request-time expression. Possible values = REQUEST, RESPONSE, ICA_REQUEST, OTHERTCP_REQUEST, AAA_REQUEST, AAA_RESPONSE
priority	<Integer>	Read-write	Integer specifying the policy's priority. The lower the number, the higher the priority. Policies are evaluated in the order of their priority numbers. Maximum value for default syntax policies is 2147483647 and for classic policies is 64000. Minimum value = 0

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum value = 2147483647
name	<String>	Read-write	Name of the virtual server. Minimum length = 1
secondary	<Boolean>	Read-write	Binds the authentication policy as the secondary policy to use in a two-factor configuration. A user must then authenticate not only via a primary authentication method but also via a secondary authentication method. User groups are aggregated across both. The user name must be exactly the same for both authentication methods, but they can require different passwords.
groupextraction	<Boolean>	Read-write	Binds the authentication policy to a tertiary chain which will be used only for group extraction. The user will not authenticate against this server, and this will only be called if primary and/or secondary

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			authentication has succeeded.
gotopriorityexpression	<String>	Read-write	Next priority expression.
policy	<String>	Read-write	The name of the policy, if any, bound to the VPN virtual server.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/vpnvserver_cspolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"vpnvserver_cspolicy_binding":{

<b>"name":<String_value>,

</b>"policy":<String_value>,

"priority":<Integer_value>,

"secondary":<Boolean_value>,

"groupextraction":<Boolean_value>,

"gotopriorityexpression":<String_value>,

"bindpoint":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_cspolicy_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_cspolicy_binding/ name_value<String> ? **args=policy: <String_value> ,secondary: <Boolean_value> ,groupextraction: <Boolean_value> ,bindpoint: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_cspolicy_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_cspolicy_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of vpnvserver_cspolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_cspolicy_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vpnvserver_cspolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnvserver_cspolicy_binding": [ {

"bindpoint":<String_value>,

"priority":<Integer_value>,

"name":<String_value>,

"secondary":<Boolean_value>,

"groupextraction":<Boolean_value>,

"gotopriorityexpression":<String_value>,

"policy":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_cspolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_cspolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnvserver_cspolicy_binding": [ {

"bindpoint":<String_value>,

"priority":<Integer_value>,

"name":<String_value>,

"secondary":<Boolean_value>,

"groupextraction":<Boolean_value>,

"gotopriorityexpression":<String_value>,

"policy":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_cspolicy_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"vpnvserver_cspolicy_binding": [ { "__count": "#no"} ] }
```

vpnvserver_feopolicy_binding

Binding object showing the feopolicy that can be bound to vpnvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
bindpoint	<String>	Read-write	Bindpoint to which the policy is bound. Possible values = REQUEST, RESPONSE, ICA_REQUEST, OTHERTCP_REQUEST, AAA_REQUEST, AAA_RESPONSE
priority	<Integer>	Read-write	Integer specifying the policy's priority. The lower the number, the higher the priority. Policies are evaluated in the order of their priority numbers. Maximum value for default syntax policies is

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			2147483647 and for classic policies is 64000. Minimum value = 0 Maximum value = 2147483647
secondary	<Boolean>	Read-write	Binds the authentication policy as the secondary policy to use in a two-factor configuration. A user must then authenticate not only via a primary authentication method but also via a secondary authentication method. User groups are aggregated across both. The user name must be exactly the same for both authentication methods, but they can require different passwords.
name	<String>	Read-write	Name of the virtual server. Minimum length = 1
groupextraction	<Boolean>	Read-write	Binds the authentication policy to a tertiary chain which will be used only for group extraction. The user

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			will not authenticate against this server, and this will only be called if primary and/or secondary authentication has succeeded.
policy	<String>	Read-write	Name of a policy to bind to the virtual server (for example, the name of an authentication, session, or endpoint analysis policy). Minimum length = 1
gotopriorityexpression	<String>	Read-write	Next priority expression.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/vpnvserver_feopolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"vpnvserver_feopolicy_binding":{

<b>"name":<String_value>,

</b>"policy":<String_value>,

"priority":<Integer_value>,

"secondary":<Boolean_value>,
```

```
"groupextraction":<Boolean_value>,

"gotopriorityexpression":<String_value>,

"bindpoint":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_feopolicy_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_feopolicy_binding/ name_value<String> ? **args=policy: <String_value> ,secondary: <Boolean_value> ,groupextraction: <Boolean_value> ,bindpoint: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_feopolicy_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_feopolicy_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of vpnvserver_feopolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_feopolicy_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vpnvserver_feopolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnvserver_feopolicy_binding": [ {

"bindpoint":<String_value>,

"priority":<Integer_value>,

"secondary":<Boolean_value>,

"name":<String_value>,

"groupextraction":<Boolean_value>,

"policy":<String_value>,

"gotopriorityexpression":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_feopolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_feopolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnvserver_feopolicy_binding": [ {

"bindpoint":<String_value>,

"priority":<Integer_value>,

"secondary":<Boolean_value>,

"name":<String_value>,

"groupextraction":<Boolean_value>,

"policy":<String_value>,

"gotopriorityexpression":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_feopolicy_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"vpnvserver_feopolicy_binding": [ { "__count": "#no"} ] }
```

vpnvserver_icapolicy_binding

Binding object showing the icapolicy that can be bound to vpnvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
groupextraction	<Boolean>	Read-write	Binds the authentication policy to a tertiary chain which will be used only for group extraction. The user will not authenticate against this server, and this will only be called if primary and/

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			or secondary authentication has succeeded.
gotopriorityexpression	<String>	Read-write	Next priority expression.
policy	<String>	Read-write	The name of the policy, if any, bound to the VPN virtual server.
bindpoint	<String>	Read-write	Bind point to which to bind the policy. Applies only to rewrite and cache policies. If you do not set this parameter, the policy is bound to REQ_DEFAULT or RES_DEFAULT, depending on whether the policy rule is a response-time or a request-time expression. Possible values = REQUEST, RESPONSE, ICA_REQUEST, OTHERTCP_REQUEST, AAA_REQUEST, AAA_RESPONSE
priority	<Integer>	Read-write	Integer specifying the policy's priority. The lower the number, the higher the priority. Policies

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			are evaluated in the order of their priority numbers. Maximum value for default syntax policies is 2147483647 and for classic policies is 64000. Minimum value = 0 Maximum value = 2147483647
name	<String>	Read-write	Name of the virtual server. Minimum length = 1
secondary	<Boolean>	Read-write	Binds the authentication policy as the secondary policy to use in a two-factor configuration. A user must then authenticate not only via a primary authentication method but also via a secondary authentication method. User groups are aggregated across both. The user name must be exactly the same for both authentication methods, but they can require different passwords.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/vpnvserver_icapolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"vpnvserver_icapolicy_binding":{

<b>"name":<String_value>,

</b>"policy":<String_value>,

"priority":<Integer_value>,

"secondary":<Boolean_value>,

"groupextraction":<Boolean_value>,

"gotopriorityexpression":<String_value>,

"bindpoint":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_icapolicy_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_icapolicy_binding/ name_value<String> ? **args=policy: <String_value> ,secondary: <Boolean_value> ,groupextraction: <Boolean_value> ,bindpoint: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_icapolicy_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_icapolicy_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of vpnvserver_icapolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_icapolicy_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vpnvserver_icapolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnvserver_icapolicy_binding": [ {

"groupextraction":<Boolean_value>,

"gotopriorityexpression":<String_value>,
```

```
"policy":<String_value>,

"bindpoint":<String_value>,

"priority":<Integer_value>,

"name":<String_value>,

"secondary":<Boolean_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_icapolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_icapolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnvserver_icapolicy_binding": [ {

"groupextraction":<Boolean_value>,

"gotopriorityexpression":<String_value>,

"policy":<String_value>,

"bindpoint":<String_value>,

"priority":<Integer_value>,

"name":<String_value>,

"secondary":<Boolean_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_icapolicy_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"vpnvserver_icapolicy_binding": [ { "__count": "#no"} ] }
```

vpnvserver_intranetip6_binding

Binding object showing the intranetip6 that can be bound to vpnvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
intranetip6	<String>	Read-write	The network id for the range of intranet IP6 addresses or individual intranet ip to be bound to the vserver.
name	<String>	Read-write	Name of the virtual server. Minimum length = 1
numaddr	<Integer>	Read-write	The number of ipv6 addresses.
acttype	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/vpnvserver_intranetip6_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"vpnvserver_intranetip6_binding":{

<b>"name":<String_value>,

</b>"intranetip6":<String_value>,

"numaddr":<Integer_value>
```

```
}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_intranetip6_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_intranetip6_binding/ name_value<String> ? **args=intranetip6: <String_value> ,numaddr: <Integer_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_intranetip6_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_intranetip6_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of vpnvserver_intranetip6_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_intranetip6_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vpnvserver_intranetip6_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnvserver_intranetip6_binding": [ {

"intranetip6":<String_value>,

"name":<String_value>,

"numaddr":<Integer_value>,

"acttype":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_intranetip6_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_intranetip6_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnvserver_intranetip6_binding": [ {

"intranetip6":<String_value>,

"name":<String_value>,

"numaddr":<Integer_value>,

"acttype":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_intranetip6_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"vpnvserver_intranetip6_binding": [ { "__count": "#no"} ] }
```

vpnvserver_intranetip_binding

Binding object showing the intranetip that can be bound to vpnvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
intranetip	<String>	Read-write	The network ID for the range of intranet IP addresses or individual intranet IP addresses to be bound to the virtual server.
name	<String>	Read-write	Name of the virtual server. Minimum length = 1
netmask	<String>	Read-write	The netmask of the intranet IP address or range.
map	<String>	Read-only	Whether or not mapped IP addresses are ON or OFF. Mapped IP addresses are source IP addresses for the virtual servers running on the Citrix ADC. Mapped IP addresses are used by the system to connect to the backend servers.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ON, OFF
acttype	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/vpnvserver_intranetip_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"vpnvserver_intranetip_binding":{

<b>"name":<String_value>,

</b>"intranetip":<String_value>,

"netmask":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_intranetip_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_intranetip_binding/ name_value<String> ? **args=intranetip: <String_value> ,netmask: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_intranetip_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_intranetip_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of vpnvserver_intranetip_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_intranetip_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vpnvserver_intranetip_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnvserver_intranetip_binding": [ {

"intranetip":<String_value>,
```

```
"name":<String_value>,

"netmask":<String_value>,

"map":<String_value>,

"acttype":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_intranetip_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_intranetip_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnvserver_intranetip_binding": [ {

"intranetip":<String_value>,
```

```
"name":<String_value>,

"netmask":<String_value>,

"map":<String_value>,

"acttype":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_intranetip_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"vpnvserver_intranetip_binding": [ { "__count": "#no"} ] }
```

vpnvserver_responderpolicy_binding

Binding object showing the responderpolicy that can be bound to vpnvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
secondary	<Boolean>	Read-write	Binds the authentication policy as the secondary policy to use in a two-factor configuration. A user must then authenticate not only via a primary authentication method but also via a secondary authentication method. User groups are aggregated across both. The user name must be exactly the same for both authentication methods, but they can require different passwords.
name	<String>	Read-write	Name of the virtual server. Minimum length = 1
priority	<Integer>	Read-write	Integer specifying the policy's priority. The lower the number, the higher the priority. Policies are evaluated in the order of their priority numbers. Maximum value for default syntax policies is 2147483647 and for classic policies is 64000.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum value = 0 Maximum value = 2147483647
bindpoint	<String>	Read-write	Bindpoint to which the policy is bound. Possible values = REQUEST, RESPONSE, ICA_REQUEST, OTHERTCP_REQUEST, AAA_REQUEST, AAA_RESPONSE
groupextraction	<Boolean>	Read-write	Binds the authentication policy to a tertiary chain which will be used only for group extraction. The user will not authenticate against this server, and this will only be called if primary and/or secondary authentication has succeeded.
policy	<String>	Read-write	The name of the policy, if any, bound to the VPN virtual server.
gotopriorityexpression	<String>	Read-write	Next priority expression.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/vpnvserver_responderpolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"vpnvserver_responderpolicy_binding":{

<b>"name":<String_value>,

</b>"policy":<String_value>,

"priority":<Integer_value>,

"secondary":<Boolean_value>,

"groupextraction":<Boolean_value>,

"gotopriorityexpression":<String_value>,

"bindpoint":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_responderpolicy_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_responderpolicy_binding/ name_value<String> ? **args=policy: <String_value> ,secondary: <Boolean_value> ,groupextraction: <Boolean_value> ,bindpoint: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_responderpolicy_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_responderpolicy_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of vpnvserver_responderpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_responderpolicy_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vpnvserver_responderpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnvserver_responderpolicy_binding": [ {

"secondary":<Boolean_value>,
```

```
"name":<String_value>,

"priority":<Integer_value>,

"bindpoint":<String_value>,

"groupextraction":<Boolean_value>,

"policy":<String_value>,

"gotopriorityexpression":<String_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_responderpolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_responderpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnvserver_responderpolicy_binding": [ {

"secondary":<Boolean_value>,

"name":<String_value>,

"priority":<Integer_value>,

"bindpoint":<String_value>,

"groupextraction":<Boolean_value>,

"policy":<String_value>,

"gotopriorityexpression":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_responderpolicy_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"vpnvserver_responderpolicy_binding": [ { "__count": "#no"} ] }
```

vpnvserver_rewritepolicy_binding

Binding object showing the rewritepolicy that can be bound to vpnvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
gotopriorityexpression	<String>	Read-write	Next priority expression.
policy	<String>	Read-write	The name of the policy, if any, bound to the VPN virtual server.
groupextraction	<Boolean>	Read-write	Binds the authentication policy to a tertiary chain which will be used only for group extraction. The user will not authenticate against this server, and this will only be called if primary and/or secondary authentication has succeeded.
priority	<Integer>	Read-write	Integer specifying the policy's priority. The lower the number, the higher the priority. Policies are evaluated in the order of their priority numbers. Maximum value for default syntax policies is 2147483647 and for

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			classic policies is 64000. Minimum value = 0 Maximum value = 2147483647
bindpoint	<String>	Read-write	Bindpoint to which the policy is bound. Possible values = REQUEST, RESPONSE, ICA_REQUEST, OTHERTCP_REQUEST, AAA_REQUEST, AAA_RESPONSE
name	<String>	Read-write	Name of the virtual server. Minimum length = 1
secondary	<Boolean>	Read-write	Binds the authentication policy as the secondary policy to use in a two-factor configuration. A user must then authenticate not only via a primary authentication method but also via a secondary authentication method. User groups are aggregated across both. The user name must be exactly the same for

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			both authentication methods, but they can require different passwords.
__count	<Double>	Read-write	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/vpnvserver_rewritepolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"vpnvserver_rewritepolicy_binding":{

<b>"name":<String_value>,

</b>"policy":<String_value>,

"priority":<Integer_value>,

"secondary":<Boolean_value>,

"groupextraction":<Boolean_value>,

"gotopriorityexpression":<String_value>,

"bindpoint":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_rewritepolicy_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_rewritepolicy_binding/ name_value<String> ? **args=policy: <String_value> ,secondary: <Boolean_value> ,groupextraction: <Boolean_value> ,bindpoint: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_rewritepolicy_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_rewritepolicy_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of vpnvserver_rewritepolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_rewritepolicy_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vpnvserver_rewritepolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnvserver_rewritepolicy_binding": [ {

"gotopriorityexpression":<String_value>,

"policy":<String_value>,

"groupextraction":<Boolean_value>,

"priority":<Integer_value>,

"bindpoint":<String_value>,

"name":<String_value>,

"secondary":<Boolean_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_rewritepolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_rewritepolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnvserver_rewritepolicy_binding": [ {

"gotopriorityexpression":<String_value>,

"policy":<String_value>,

"groupextraction":<Boolean_value>,

"priority":<Integer_value>,

"bindpoint":<String_value>,

"name":<String_value>,

"secondary":<Boolean_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_rewritepolicy_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"vpnvserver_rewritepolicy_binding": [ { "__count": "#no"} ] }
```

vpnvserver_secureprivateaccessurl_binding

Binding object showing the secureprivateaccessurl that can be bound to vpnvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the virtual server. Minimum length = 1
secureprivateaccessurl	<String>	Read-write	Configured Secure Private Access URL.
acttype	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/vpnvserver_secureprivateaccessurl_binding
HTTP Method: PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"vpnvserver_secureprivateaccessurl_binding":{

<b>"name":<String_value>,
```

```
</b>"secureprivateaccessurl":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_secureprivateaccessurl_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_secureprivateaccessurl_binding/ name_value<String> ? **args=secureprivateaccessurl: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_secureprivateaccessurl_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_secureprivateaccessurl_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of vpnvserver_secureprivateaccessurl_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_secureprivateaccessurl_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vpnvserver_secureprivateaccessurl_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnvserver_secureprivateaccessurl_binding": [ {

"name":<String_value>,

"secureprivateaccessurl":<String_value>,

"acttype":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_secureprivateaccessurl_binding
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_secureprivateaccessurl_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnvserver_secureprivateaccessurl_binding": [ {

"name":<String_value>,

"secureprivateaccessurl":<String_value>,

"acttype":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_secureprivateaccessurl_binding/name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"vpnvserver_secureprivateaccessurl_binding": [ { "__count": "#no"} ] }
```

vpnvserver_sharefileserver_binding

Binding object showing the sharefileserver that can be bound to vpnvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the virtual server. Minimum length = 1
sharefile	<String>	Read-write	Configured ShareFile server in XenMobile deployment. Format IP:PORT / FQDN:PORT.
acttype	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/vpnvserver_sharefileserver_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"vpnvserver_sharefileserver_binding":{

<b>"name":<String_value>,

</b>"sharefile":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_sharefileserver_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_sharefileserver_binding/ name_value<String> ? **args=sharefile: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_sharefileserver_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_sharefileserver_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of vpnvserver_sharefileserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_sharefileserver_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vpnvserver_sharefileserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnvserver_sharefileserver_binding": [ {

"name":<String_value>,

"sharefile":<String_value>,

"acttype":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_sharefileserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_sharefileserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnvserver_sharefileserver_binding": [ {

"name":<String_value>,

"sharefile":<String_value>,

"acttype":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_sharefileserver_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"vpnvserver_sharefileserver_binding": [ { "__count": "#no"} ] }
```

vpnvserver_staserver_binding

Binding object showing the staserver that can be bound to vpnvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
staserver	<String>	Read-write	Configured Secure Ticketing Authority (STA) server.
staaddresstype	<String>	Read-write	Type of the STA server address(ipv4/v6). Possible values = IPV4, IPV6
name	<String>	Read-write	Name of the virtual server. Minimum length = 1
stastate	<String>	Read-only	State of the STA Server. If Authority ID is set then STA Server is UP else DOWN. Possible values = UP, DOWN
acttype	<Integer>	Read-only	.
staauthid	<String>	Read-only	Authority ID of the STA Server. Authority ID is used to match incoming STA tickets in the SOCKS/CGP protocol with the right STA server.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/vpnvserver_staserver_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"vpnvserver_staserver_binding":{

<b>"name":<String_value>,

</b>"staserver":<String_value>,

"staaddresstype":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_staserver_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_staserver_binding/ name_value<String> ? **args=staserver: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_staserver_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/

vpnvserver_staserver_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of vpnvserver_staserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_staserver_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vpnvserver_staserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnvserver_staserver_binding": [ {

"staserver":<String_value>,

"staaddresstype":<String_value>,

"name":<String_value>,

"stastate":<String_value>,

"acttype":<Integer_value>,

"staauthid":<String_value>
```

```
}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_staserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_staserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnvserver_staserver_binding": [ {

"staserver":<String_value>,

"staaddresstype":<String_value>,

"name":<String_value>,

"stastate":<String_value>,

"acttype":<Integer_value>,
```

```
"staauthid":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_staserver_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"vpnvserver_staserver_binding": [ { "__count": "#no"} ] }
```

vpnvserver_vpnclientlessaccesspolicy_binding

Binding object showing the vpnclientlessaccesspolicy that can be bound to vpnvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the virtual server. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
secondary	<Boolean>	Read-write	Binds the authentication policy as the secondary policy to use in a two-factor configuration. A user must then authenticate not only via a primary authentication method but also via a secondary authentication method. User groups are aggregated across both. The user name must be exactly the same for both authentication methods, but they can require different passwords.
priority	<Integer>	Read-write	Integer specifying the policy's priority. The lower the number, the higher the priority. Policies are evaluated in the order of their priority numbers. Maximum value for default syntax policies is 2147483647 and for classic policies is 64000. Minimum value = 0 Maximum value = 2147483647

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
bindpoint	<String>	Read-write	Bindpoint to which the policy is bound. Possible values = REQUEST, RESPONSE, ICA_REQUEST, OTHERTCP_REQUEST, AAA_REQUEST, AAA_RESPONSE
gotopriorityexpression	<String>	Read-write	Next priority expression.
policy	<String>	Read-write	The name of the policy, if any, bound to the VPN virtual server.
groupextraction	<Boolean>	Read-write	Binds the authentication policy to a tertiary chain which will be used only for group extraction. The user will not authenticate against this server, and this will only be called if primary and/or secondary authentication has succeeded.
acttype	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/vpnvserver_vpnclientlessaccesspolicy_binding
HTTP Method: PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"vpnvserver_vpnclientlessaccesspolicy_binding":{

<b>"name":<String_value>,

</b>"policy":<String_value>,

"priority":<Integer_value>,

"secondary":<Boolean_value>,

"groupextraction":<Boolean_value>,

"gotopriorityexpression":<String_value>,

"bindpoint":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_vpnclientlessaccesspolicy_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_vpnclientlessaccesspolicy_binding/ name_value<String> ? **args=policy: <String_value> ,secondary: <Boolean_value> ,groupextraction: <Boolean_value> ,bindpoint: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_vpnclientlessaccesspolicy_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_vpnclientlessaccesspolicy_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of vpnvserver_vpnclientlessaccesspolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_vpnclientlessaccesspolicy_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vpnvserver_vpnclientlessaccesspolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnvserver_vpnclientlessaccesspolicy_binding": [ {

"name":<String_value>,
```

```
"secondary":<Boolean_value>,

"priority":<Integer_value>,

"bindpoint":<String_value>,

"gotopriorityexpression":<String_value>,

"policy":<String_value>,

"groupextraction":<Boolean_value>,

"acttype":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_vpnclientlessaccesspolicy_binding
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_vpnclientlessaccesspolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnvserver_vpnclientlessaccesspolicy_binding": [ {

"name":<String_value>,

"secondary":<Boolean_value>,

"priority":<Integer_value>,

"bindpoint":<String_value>,

"gotopriorityexpression":<String_value>,

"policy":<String_value>,

"groupextraction":<Boolean_value>,

"acttype":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_vpnclientlessaccesspolicy_binding/name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"vpnvserver_vpnclientlessaccesspolicy_binding": [ { "__count": "#no"} ] }
```

vpnvserver_vpnepaprofile_binding

Binding object showing the vpnepaprofile that can be bound to vpnvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
epaprofileoptional	<Boolean>	Read-write	Mark the EPA profile optional for preauthentication EPA profile. User would be shown a logon page even if the EPA profile fails to evaluate.
name	<String>	Read-write	Name of the virtual server. Minimum length = 1
epaprofile	<String>	Read-write	Advanced EPA profile to bind.
acttype	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/vpnvserver_vpnepaprofile_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"vpnvserver_vpnepaprofile_binding":{
```

```
<b>"name":<String_value>,

</b>"epaprofile":<String_value>,

"epaprofileoptional":<Boolean_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_vpnepaprofile_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_vpnepaprofile_binding/ name_value<String> ? **args=epaprofile: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_vpnepaprofile_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_vpnepaprofile_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of vpnvserver_vpnepaprofile_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_vpnepaprofile_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vpnvserver_vpnepaprofile_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnvserver_vpnepaprofile_binding": [ {

"epaprofileoptional":<Boolean_value>,

"name":<String_value>,

"epaprofile":<String_value>,

"acttype":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_vpnepaprofile_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_vpnepaprofile_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnvserver_vpnepaprofile_binding": [ {

"epaprofileoptional":<Boolean_value>,

"name":<String_value>,

"epaprofile":<String_value>,

"acttype":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_vpnepaprofile_binding/name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"vpnvserver_vpnepaprofile_binding": [ { "__count": "#no"} ] }
```

vpnvserver_vpneula_binding

Binding object showing the vpneula that can be bound to vpnvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the virtual server. Minimum length = 1
eula	<String>	Read-write	Name of the EULA bound to VPN vserver.
acttype	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)

- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/vpnvserver_vpneula_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"vpnvserver_vpneula_binding":{

<b>"name":<String_value>,

</b>"eula":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_vpneula_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_vpneula_binding/ name_value<String> ? **args=eula: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_vpneula_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_vpneula_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of vpnvserver_vpneula_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_vpneula_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vpnvserver_vpneula_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnvserver_vpneula_binding": [ {

"name":<String_value>,

"eula":<String_value>,

"acttype":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_vpneula_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_vpneula_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnvserver_vpneula_binding": [ {

"name":<String_value>,

"eula":<String_value>,

"acttype":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_vpneula_binding/name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"vpnvserver_vpneula_binding": [ { "__count": "#no"} ] }
```

vpnvserver_vpnintranetapplication_binding

Binding object showing the vpnintranetapplication that can be bound to vpnvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the virtual server. Minimum length = 1
intranetapplication	<String>	Read-write	The intranet VPN application.
acttype	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/vpnvserver_vpnintranetapplication_binding
HTTP Method: PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"vpnvserver_vpnintranetapplication_binding":{

<b>"name":<String_value>,
```

```
</b>"intranetapplication":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_vpnintranetapplication_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_vpnintranetapplication_binding/ name_value<String> ? **args=intranetapplication: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_vpnintranetapplication_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_vpnintranetapplication_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of vpnvserver_vpnintranetapplication_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_vpnintranetapplication_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vpnvserver_vpnintranetapplication_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnvserver_vpnintranetapplication_binding": [ {

"name":<String_value>,

"intranetapplication":<String_value>,

"acttype":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_vpnintranetapplication_binding
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_vpnintranetapplication_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnvserver_vpnintranetapplication_binding": [ {

"name":<String_value>,

"intranetapplication":<String_value>,

"acttype":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_vpnintranetapplication_binding/name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"vpnvserver_vpnintranetapplication_binding": [ { "__count": "#no"} ] }
```

vpnvserver_vpnnexthopserver_binding

Binding object showing the vpnnexthopserver that can be bound to vpnvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the virtual server. Minimum length = 1
nexthopserver	<String>	Read-write	The name of the next hop server bound to the VPN virtual server.
acttype	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/vpnvserver_vpnnexthopserver_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"vpnvserver_vpnnexthopserver_binding":{

<b>"name":<String_value>,

</b>"nexthopserver":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_vpnnexthopserver_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_vpnnexthopserver_binding/ name_value<String> ? **args=nexthopserver: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_vpnnexthopserver_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_vpnnexthopserver_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of vpnvserver_vpnnexthopserver_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_vpnnexthopserver_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vpnvserver_vpnnexthopserver_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnvserver_vpnnexthopserver_binding": [ {

"name":<String_value>,

"nexthopserver":<String_value>,

"acttype":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_vpnnexthopserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_vpnnexthopserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnvserver_vpnnexthopserver_binding": [ {

"name":<String_value>,

"nexthopserver":<String_value>,

"acttype":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_vpnnexthopserver_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"vpnvserver_vpnnexthopserver_binding": [ { "__count": "#no"} ] }
```

vpnvserver_vpnportaltheme_binding

Binding object showing the vpnportaltheme that can be bound to vpnvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
portaltheme	<String>	Read-write	Name of the portal theme bound to VPN vserver.
name	<String>	Read-write	Name of the virtual server. Minimum length = 1
acttype	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/vpnvserver_vpnportaltheme_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"vpnvserver_vpnportaltheme_binding":{

<b>"name":<String_value>,

</b>"portaltheme":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_vpnportaltheme_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_vpnportaltheme_binding/ name_value<String> ? **args=portaltheme: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_vpnportaltheme_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_vpnportaltheme_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of vpnvserver_vpnportaltheme_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_vpnportaltheme_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vpnvserver_vpnportaltheme_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnvserver_vpnportaltheme_binding": [ {

"portaltheme":<String_value>,

"name":<String_value>,

"acttype":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_vpnportaltheme_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_vpnportaltheme_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnvserver_vpnportaltheme_binding": [ {

"portaltheme":<String_value>,

"name":<String_value>,

"acttype":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_vpnportaltheme_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"vpnvserver_vpnportaltheme_binding": [ { "__count": "#no"} ] }
```

vpnvserver_vpnsecureprivateaccessprofile_binding

Binding object showing the vpnsecureprivateaccessprofile that can be bound to vpnvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
secureprivateaccessprofile	<String>	Read-write	Name of the Secure Private Access profile bound to the vserver. Minimum length = 1 Maximum length = 31
name	<String>	Read-write	Name of the virtual server. Minimum length = 1
acttype	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/ vpnvserver_vpnsecureprivateaccessprofile_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"vpnvserver_vpnsecureprivateaccessprofile_binding":{

<b>"name":<String_value>,

</b>"secureprivateaccessprofile":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_vpnsecureprivateaccessprofile_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_vpnsecureprivateaccessprofile_binding/ name_value<String> ? **args=secureprivateaccessprofile: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_vpnsecureprivateaccessprofile_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_vpnsecureprivateaccessprofile_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of vpnvserver_vpnsecureprivateaccessprofile_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_vpnsecureprivateaccessprofile_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vpnvserver_vpnsecureprivateaccessprofile_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnvserver_vpnsecureprivateaccessprofile_binding": [ {

"secureprivateaccessprofile":<String_value>,

"name":<String_value>,

"acttype":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_vpnsecureprivateaccessprofile_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_vpnsecureprivateaccessprofile_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnvserver_vpnsecureprivateaccessprofile_binding": [ {

"secureprivateaccessprofile":<String_value>,

"name":<String_value>,

"acttype":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_vpnsecureprivateaccessprofile_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"vpnvserver_vpnsecureprivateaccessprofile_binding": [ { "__count":
"#no"} ] }
```

vpnvserver_vpnsessionpolicy_binding

Binding object showing the vpnsessionpolicy that can be bound to vpnvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
priority	<Integer>	Read-write	Integer specifying the policy's priority. The lower the number, the higher the priority. Policies are evaluated in the order of their priority numbers. Maximum value for default syntax policies is 2147483647 and for classic policies is 64000. Minimum value = 0 Maximum value = 2147483647
bindpoint	<String>	Read-write	Bind point to which to bind the policy. Applies only to rewrite and cache policies. If you do not set this parameter, the policy is bound to REQ_DEFAULT or RES_DEFAULT, depending on whether the policy

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			rule is a response-time or a request-time expression. Possible values = REQUEST, RESPONSE, ICA_REQUEST, OTHERTCP_REQUEST, AAA_REQUEST, AAA_RESPONSE
secondary	<Boolean>	Read-write	Binds the authentication policy as the secondary policy to use in a two-factor configuration. A user must then authenticate not only via a primary authentication method but also via a secondary authentication method. User groups are aggregated across both. The user name must be exactly the same for both authentication methods, but they can require different passwords.
name	<String>	Read-write	Name of the virtual server. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
policy	<String>	Read-write	The name of the policy, if any, bound to the VPN virtual server.
gotopriorityexpression	<String>	Read-write	Applicable only to advance vpn session policy. Expression or other value specifying the next policy to evaluate if the current policy evaluates to TRUE. Specify one of the following values: * NEXT - Evaluate the policy with the next higher priority number. * END - End policy evaluation. * An expression that evaluates to a number. If you specify an expression, the number to which it evaluates determines the next policy to evaluate, as follows: * If the expression evaluates to a higher numbered priority, the policy with that priority is evaluated next. * If the expression evaluates to the priority of the current policy, the policy with the next higher numbered

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			priority is evaluated next. * If the expression evaluates to a number that is larger than the largest numbered priority, policy evaluation ends. An UNDEF event is triggered if: * The expression is invalid. * The expression evaluates to a priority number that is numerically lower than the current policy's priority. * The expression evaluates to a priority number that is between the current policy's priority number (say, 30) and the highest priority number (say, 100), but does not match any configured priority number (for example, the expression evaluates to the number 85). This example assumes that the priority number increments by 10 for every successive policy, and therefore a priority number of 85 does not exist in the policy label.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
groupextraction	<Boolean>	Read-write	Binds the authentication policy to a tertiary chain which will be used only for group extraction. The user will not authenticate against this server, and this will only be called if primary and/or secondary authentication has succeeded.
acttype	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/vpnvserver_vpnsessionpolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"vpnvserver_vpnsessionpolicy_binding":{

<b>"name":<String_value>,

</b>"policy":<String_value>,

"priority":<Integer_value>,

"secondary":<Boolean_value>,

"groupextraction":<Boolean_value>,
```

```
"gotopriorityexpression":<String_value>,

"bindpoint":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_vpnsessionpolicy_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_vpnsessionpolicy_binding/ name_value<String> ? **args=policy: <String_value> ,secondary: <Boolean_value> ,groupextraction: <Boolean_value> ,bindpoint: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_vpnsessionpolicy_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_vpnsessionpolicy_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of vpnvserver_vpnsessionpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_vpnsessionpolicy_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vpnvserver_vpnsessionpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnvserver_vpnsessionpolicy_binding": [ {

"priority":<Integer_value>,

"bindpoint":<String_value>,

"secondary":<Boolean_value>,

"name":<String_value>,

"policy":<String_value>,

"gotopriorityexpression":<String_value>,

"groupextraction":<Boolean_value>,

"acttype":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_vpnsessionpolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_vpnsessionpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnvserver_vpnsessionpolicy_binding": [ {

"priority":<Integer_value>,

"bindpoint":<String_value>,

"secondary":<Boolean_value>,

"name":<String_value>,

"policy":<String_value>,

"gotopriorityexpression":<String_value>,

"groupextraction":<Boolean_value>,
```

```
"acttype":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_vpnsessionpolicy_binding/name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"vpnvserver_vpnsessionpolicy_binding": [ { "__count": "#no"} ] }
```

vpnvserver_vpntrafficpolicy_binding

Binding object showing the vpntrafficpolicy that can be bound to vpnvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
groupextraction	<Boolean>	Read-write	Binds the authentication policy to a tertiary chain which will be used

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			only for group extraction. The user will not authenticate against this server, and this will only be called if primary and/or secondary authentication has succeeded.
policy	<String>	Read-write	The name of the policy, if any, bound to the VPN virtual server.
gotopriorityexpression	<String>	Read-write	Applicable only to advance vpn session policy. Expression or other value specifying the next policy to evaluate if the current policy evaluates to TRUE. Specify one of the following values: * NEXT - Evaluate the policy with the next higher priority number. * END - End policy evaluation. * An expression that evaluates to a number. If you specify an expression, the number to which it evaluates determines the next policy to evaluate, as follows: * If the expression evaluates

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			to a higher numbered priority, the policy with that priority is evaluated next. * If the expression evaluates to the priority of the current policy, the policy with the next higher numbered priority is evaluated next. * If the expression evaluates to a number that is larger than the largest numbered priority, policy evaluation ends. An UNDEF event is triggered if: * The expression is invalid. * The expression evaluates to a priority number that is numerically lower than the current policy's priority. * The expression evaluates to a priority number that is between the current policy's priority number (say, 30) and the highest priority number (say, 100), but does not match any configured priority number (for example, the expression evaluates to the number 85).

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			This example assumes that the priority number increments by 10 for every successive policy, and therefore a priority number of 85 does not exist in the policy label.
secondary	<Boolean>	Read-write	Binds the authentication policy as the secondary policy to use in a two-factor configuration. A user must then authenticate not only via a primary authentication method but also via a secondary authentication method. User groups are aggregated across both. The user name must be exactly the same for both authentication methods, but they can require different passwords.
name	<String>	Read-write	Name of the virtual server. Minimum length = 1
priority	<Integer>	Read-write	Integer specifying the policy's priority. The lower the number, the higher

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			the priority. Policies are evaluated in the order of their priority numbers. Maximum value for default syntax policies is 2147483647 and for classic policies is 64000. Minimum value = 0 Maximum value = 2147483647
bindpoint	<String>	Read-write	Bind point to which to bind the policy. Applies only to rewrite and cache policies. If you do not set this parameter, the policy is bound to REQ_DEFAULT or RES_DEFAULT, depending on whether the policy rule is a response-time or a request-time expression. Possible values = REQUEST, RESPONSE, ICA_REQUEST, OTHERTCP_REQUEST, AAA_REQUEST, AAA_RESPONSE
acttype	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/vpnvserver_vpntrafficpolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"vpnvserver_vpntrafficpolicy_binding":{

<b>"name":<String_value>,

</b>"policy":<String_value>,

"priority":<Integer_value>,

"secondary":<Boolean_value>,

"groupextraction":<Boolean_value>,

"gotopriorityexpression":<String_value>,

"bindpoint":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_vpntrafficpolicy_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_vpntrafficpolicy_binding/ name_value<String> ? **args=policy: <String_value> ,secondary: <Boolean_value> ,groupextraction: <Boolean_value> ,bindpoint: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_vpntrafficpolicy_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_vpntrafficpolicy_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of vpnvserver_vpntrafficpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_vpntrafficpolicy_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vpnvserver_vpntrafficpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnvserver_vpntrafficpolicy_binding": [ {

"groupextraction":<Boolean_value>,
```

```
"policy":<String_value>,

"gotopriorityexpression":<String_value>,

"secondary":<Boolean_value>,

"name":<String_value>,

"priority":<Integer_value>,

"bindpoint":<String_value>,

"acttype":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_vpntrafficpolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_vpntrafficpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnvserver_vpntrafficpolicy_binding": [ {

"groupextraction":<Boolean_value>,

"policy":<String_value>,

"gotopriorityexpression":<String_value>,

"secondary":<Boolean_value>,

"name":<String_value>,

"priority":<Integer_value>,

"bindpoint":<String_value>,

"acttype":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_vpntrafficpolicy_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"vpnvserver_vpntrafficpolicy_binding": [ { "__count": "#no"} ] }
```

vpnvserver_vpnurl_binding

Binding object showing the vpnurl that can be bound to vpnvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
urlname	<String>	Read-write	The intranet URL.
name	<String>	Read-write	Name of the virtual server. Minimum length = 1
acttype	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/vpnvserver_vpnurl_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"vpnvserver_vpnurl_binding":{

<b>"name":<String_value>,

</b>"urlname":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_vpnurl_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_vpnurl_binding/ name_value<String> ? **args=urlname: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_vpnurl_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_vpnurl_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of vpnvserver_vpnurl_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_vpnurl_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vpnvserver_vpnurl_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnvserver_vpnurl_binding": [ {

"urlname":<String_value>,

"name":<String_value>,

"acttype":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_vpnurl_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_vpnurl_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnvserver_vpnurl_binding": [ {

"urlname":<String_value>,

"name":<String_value>,

"acttype":<Integer_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_vpnurl_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"vpnvserver_vpnurl_binding": [ { "__count": "#no"} ] }
```

vpnvserver_vpnurlpolicy_binding

Binding object showing the vpnurlpolicy that can be bound to vpnvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
bindpoint	<String>	Read-write	Bind point to which to bind the policy. Applies only to rewrite and cache policies. If you do not set this parameter, the policy is bound to REQ_DEFAULT or RES_DEFAULT, depending on whether the policy rule is a response-time or a request-time expression. Possible values = REQUEST, RESPONSE, ICA_REQUEST, OTHERTCP_REQUEST, AAA_REQUEST, AAA_RESPONSE
priority	<Integer>	Read-write	Integer specifying the policy's priority. The lower the number, the higher the priority. Policies are evaluated in the order of their priority numbers. Maximum value for default syntax policies is 2147483647 and for classic policies is 64000.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum value = 0 Maximum value = 2147483647
secondary	<Boolean>	Read-write	Binds the authentication policy as the secondary policy to use in a two-factor configuration. A user must then authenticate not only via a primary authentication method but also via a secondary authentication method. User groups are aggregated across both. The user name must be exactly the same for both authentication methods, but they can require different passwords.
name	<String>	Read-write	Name of the virtual server. Minimum length = 1
groupextraction	<Boolean>	Read-write	Binds the authentication policy to a tertiary chain which will be used only for group extraction. The user will not authenticate against this server, and this will only be

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			called if primary and/ or secondary authentication has succeeded.
policy	<String>	Read-write	The name of the policy, if any, bound to the VPN virtual server.
gotopriorityexpression	<String>	Read-write	Next priority expression.
acttype	<Integer>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of

creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address /nitro/v1/config/vpnvserver_vpnurlpolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"vpnvserver_vpnurlpolicy_binding":{

<b>"name":<String_value>,

</b>"policy":<String_value>,

"priority":<Integer_value>,

"secondary":<Boolean_value>,

"groupextraction":<Boolean_value>,

"gotopriorityexpression":<String_value>,
```

```
"bindpoint":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_vpnurlpolicy_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_vpnurlpolicy_binding/ name_value<String> ? **args=policy: <String_value> ,secondary: <Boolean_value> ,groupextraction: <Boolean_value> ,bindpoint: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_vpnurlpolicy_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_vpnurlpolicy_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of vpnvserver_vpnurlpolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_vpnurlpolicy_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the vpnvserver_vpnurlpolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnvserver_vpnurlpolicy_binding": [ {

"bindpoint":<String_value>,

"priority":<Integer_value>,

"secondary":<Boolean_value>,

"name":<String_value>,

"groupextraction":<Boolean_value>,

"policy":<String_value>,

"gotopriorityexpression":<String_value>,

"acttype":<Integer_value>

}]}
```

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_vpnurlpolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ vpnvserver_vpnurlpolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnvserver_vpnurlpolicy_binding": [ {

"bindpoint":<String_value>,

"priority":<Integer_value>,

"secondary":<Boolean_value>,

"name":<String_value>,

"groupextraction":<Boolean_value>,

"policy":<String_value>,

"gotopriorityexpression":<String_value>,

"acttype":<Integer_value>

}]}
```

```
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/vpnvserver_vpnurlpolicy_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"vpnvserver_vpnurlpolicy_binding": [ { "__count": "#no"} ] }
```

wasm

Wasm

WASM Module configuration.

NAME	DESCRIPTION
wasmmodule	Configuration for WASM Module

wasmmodule

Configuration for WASM Module resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	The name of the WASM module file. Minimum length = 1 Maximum length = 127
modulefile	<String>	Read-write	File name of the WASM module. Minimum length = 1 Maximum length = 255
signaturefile	<String>	Read-write	The SHA256 file contains the hash value used to validate the WASM module.. Minimum length = 1 Maximum length = 255
settingfile	<String>	Read-write	The WASM module filename contains module-specific configuration settings.
comment	<String>	Read-write	Any type of information about this WASM module.
referencecount	<Integer>	Read-only	The number of references to the wasm_module.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- UPDATE
- UNSET
- DELETE
- GET (ALL)
- GET
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

ADD

URL: http:// <netscaler-ip-address> /nitro/v1/config/wasmmodule **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"wasmmodule":{

<b>"name":<String_value>,

</b><b>"modulefile":<String_value>,

</b><b>"signaturefile":<String_value>,

</b>"settingfile":<String_value>,

"comment":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UPDATE

URL: http:// <netscaler-ip-address> /nitro/v1/config/wasmmodule **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"wasmmodule":{

<b>"name":<String_value>,

</b>"settingfile":<String_value>,
```

```
"comment":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

UNSET

URL: http:// <netscaler-ip-address> /nitro/v1/config/wasmmodule? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"wasmmodule":{

<b>"name":<String_value>,

</b>"settingfile":true,

"comment":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

DELETE

URL: http:// <netscaler-ip-address> /nitro/v1/config/wasmmodule/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/config/wasmmodule **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/wasmmodule? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/wasmmodule? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of wasmmodule resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/wasmmodule? **view=summary**

Use this query-parameter to get the summary output of wasmmodule resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/wasmmodule? **pagesize=#no;pageno=#no**

Use this query-parameter to get the wasmmodule resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "wasmmodule": [ {

"name":<String_value>,

"name":<String_value>,

"modulefile":<String_value>,

"signaturefile":<String_value>,

"settingfile":<String_value>,

"comment":<String_value>,

"referencecount":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/config/wasmmodule/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/wasmmodule/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/wasmmodule/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of wasmmodule resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "wasmmodule": [ {

"name":<String_value>,

"name":<String_value>,

"modulefile":<String_value>,

"signaturefile":<String_value>,

"settingfile":<String_value>,

"comment":<String_value>,

"referencecount":<Integer_value>,

"_nextgenapiresource":<String_value>

}]}
```

COUNT

URL: http:// <netscaler-ip-address> /nitro/v1/config/wasmmodule? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "wasmmodule": [ { "__count": "#no"} ] }
```

Statistics

The statistics API is arranged in a logical groups of objects. Choose an appropriate group to find more details.

NAME	DESCRIPTION
AAA	Authentication, authorization, and accounting service statistics.
Api	API statistics
Appflow	AppFlow statistics.
Application Firewall	Application Firewall statistics.
Appqoe	Application Level Quality of Experience statistics
Audit	Audit statistics.

NAME	DESCRIPTION
Authentication	Authentication statistics.
Authorization	Authorization statistics. Authorization services check which resources users are authorized to access, and grant permissions accordingly.
Autoscale	AutoScale statistics.
Basic	Basic system statistics.
Bot	Bot Management.
Integrated Caching	Integrated Caching statistics. The Integrated Caching feature is used to cache static and dynamic web application data.
Cloud	Citrix ADC as SD proxy statistics and cloud discovery commands.
Cluster	Cluster commands.
Compression	Compression statistics. The system's feature for compressing HTTP responses to compression-aware browsers.
CI	Content Inspection
Cache Redirection	Cache redirection statistics. The cache redirection feature can transparently redirect cacheable HTTP requests to a cache and send non-cacheable or dynamic HTTP

NAME	DESCRIPTION
	requests to the origin server. A cache stores or caches frequently requested web content and serves such web content to a client on behalf of the origin servers, alleviating the load on the origin server farm.
Content Switching	Content Switching statistics. Content Switching feature that enables you to direct traffic to servers on the basis of content.
Denylist	Denylist level statistics.
Domain Name Service	Domain Name Service(DNS) statistics.
Front-end-optimization	Front end optimization statistics. The system's feature to optimize Web content for performance.
Global Server Load Balancing	Global Server Load Balancing (GSLB) statistics. GSLB feature ensures that client requests are directed to a best performing site available in a global enterprise and distributed Internet environment.
High Availability	High-availability commands.
Ica	ICA statistics.
Insight	Insight statistics.
Ipsec	IPSEC statistics.

NAME	DESCRIPTION
Ipsecalg	IPSECALG statistics.
Load Balancing	Load Balancing statistics. The load balancing methods manage the selection of an appropriate physical server in a server farm.
LLDP	Link Layer Discovery Protocol.
Lsn	Large Scale NAT commands
Network	Networking commands.
NS	System/Global level statistics.
Pcp	Port Control Protocol statistics.
Protocol	Protocol statistics.
Qos	QoS statistics.
Rdp	RDP statistics.
Responder	Responder statistics.
Rewrite	Rewrite statistics.
SNMP	SNMP(Simple Network Management Protocol) statistics.

NAME	DESCRIPTION
Spillover	Spillover policies and actions.
SSL	SSL statistics
Stream	Stream statistics.
System	System statistics.
Traffic Management	TM session/policy statistics.
Transform	URL Transformation statistics.
Tunnel	SSL VPN Tunnel statistics.
User	User protocol statistics.
VideoOptimization	Video optimization feature is used to show (i) the stats of different media types that are being served by the Citrix ADC and (ii) the details of optimization applied on ABR videos
SSL VPN	Virtual Private Network statistics.

aaa

AAA

Authentication, authorization, and accounting service statistics.

NAME	DESCRIPTION
aaa	Statistics for aaa.

NAME	DESCRIPTION

aaa

Statistics for aaa.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full
aaaauthsuccess	<Double>	Read-only	Count of authentication successes.
aaaauthsuccessrate	<Double>	Read-only	Rate (/s) counter for aaaauthsuccess
aaaauthfail	<Double>	Read-only	Count of authentication failures.
aaaauthfailrate	<Double>	Read-only	Rate (/s) counter for aaaauthfail
aaaauthonlyhttpsuccess	<Double>	Read-only	Count of HTTP connections that succeeded authorization.
aaaauthonlyhttpsuccessrate	<Double>	Read-only	Rate (/s) counter for aaaauthonlyhttpsuccess
aaaauthonlyhttpfail	<Double>	Read-only	Count of HTTP connections that failed authorization.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
aaaauthonlyhttpfailrate	<Double>	Read-only	Rate (/s) counter for aaaauthonlyhttpfail
aaaauthnonhttpsuccess	<Double>	Read-only	Count of non HTTP connections that succeeded authorization.
aaaauthnonhttpsuccessrate	<Double>	Read-only	Rate (/s) counter for aaaauthnonhttpsuccess
aaaauthnonhttpfail	<Double>	Read-only	Count of non HTTP connections that failed authorization.
aaaauthnonhttpfailrate	<Double>	Read-only	Rate (/s) counter for aaaauthnonhttpfail
aaacursessions	<Double>	Read-only	Count of current SmartAccess AAA sessions.
aaacursessionsrate	<Double>	Read-only	Rate (/s) counter for aaacursessions
aaatotsessions	<Double>	Read-only	Count of all SmartAccess AAA sessions.
aaasessionsrate	<Double>	Read-only	Rate (/s) counter for aaatotsessions
aaatotsessiontimeout	<Double>	Read-only	Count of AAA sessions that have timed out.
aaasessiontimeoutrate	<Double>	Read-only	Rate (/s) counter for aaatotsessiontimeout

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
aaacuricasessions	<Double>	Read-only	Count of current Basic ICA only sessions.
aaacuricasessionsrate	<Double>	Read-only	Rate (/s) counter for aaacuricasessions
aaacuricaonlyconn	<Double>	Read-only	Count of current Basic ICA only connections.
aaacuricaonlyconnrate	<Double>	Read-only	Rate (/s) counter for aaacuricaonlyconn
aaacuricaconn	<Double>	Read-only	Count of current SmartAccess ICA connections.
aaacuricaconnrate	<Double>	Read-only	Rate (/s) counter for aaacuricaconn
aaacurtmsessions	<Double>	Read-only	Count of current AAATM sessions.
aaacurtmsessionsrate	<Double>	Read-only	Rate (/s) counter for aaacurtmsessions
aaatottmsessions	<Double>	Read-only	Count of all AAATM sessions.
aaatmsessionsrate	<Double>	Read-only	Rate (/s) counter for aaatottmsessions
aaatotwafblock	<Double>	Read-only	Total Number of Requests that are blocked as part of Appfw Validation for AAA
aaawafblockrate	<Double>	Read-only	Rate (/s) counter for aaatotwafblock

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
aaatmtotwafblock	<Double>	Read-only	Total Number of Requests that are blocked as part of Appfw Validation for AAATM
aaatmwafblockrate	<Double>	Read-only	Rate (/s) counter for aaatmtotwafblock

Operations

(click to see Properties)

- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/aaa **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/aaa? **args=detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get aaa resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/aaa? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "aaa": [ {

"aaaauthnonhttpfail":<Double_value>,

"aaatotsessiontimeout":<Double_value>,

"aaaauthnonhttpsuccess":<Double_value>,

"aaacuricasessions":<Double_value>,

"aaaauthonlyhttpfail":<Double_value>,

"aaatottmsessions":<Double_value>,
```

```
"aaaauthonlyhttpsuccess":<Double_value>,

"aaaauthnonhttpfailrate":<Double_value>,

"aaacuricaonlyconn":<Double_value>,

"aaatotsessions":<Double_value>,

"aaatmtotwafblock":<Double_value>,

"aaawafblockrate":<Double_value>,

"aaaauthnonhttpsuccessrate":<Double_value>,

"aaacurtmsessions":<Double_value>,

"aaacuricaconnrate":<Double_value>,

"aaaauthfailrate":<Double_value>,

"aaacuricasessionsrate":<Double_value>,

"aaasessiontimeoutrate":<Double_value>,

"aaatmsessionsrate":<Double_value>,

"aaaauthonlyhttpsuccessrate":<Double_value>,

"aaaauthfail":<Double_value>,

"aaacuricaonlyconnrate":<Double_value>,

"aaacurtmsessionsrate":<Double_value>,

"aaatotwafblock":<Double_value>,

"aaaauthsuccessrate":<Double_value>,

"aaaauthsuccess":<Double_value>,

"aaaauthonlyhttpfailrate":<Double_value>,

"aaasessionsrate":<Double_value>,
```

```
"aaatmwafblockrate":<Double_value>,

"aaacursessions":<Double_value>,

"aaacuricaconn":<Double_value>,

"aaacursessionsrate":<Double_value>

}]}
```

api

Api

API statistics

NAME	DESCRIPTION
apispec	Statistics for API specification resource.

apispec

Statistics for API specification resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the api spec for which to display stats. Minimum length = 1
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
apispechits	<Double>	Read-only	Number of received requests for the API specification.
apispechitsrate	<Double>	Read-only	Rate (/s) counter for apispechits
apispecsuccessfullyvalidated	<Double>	Read-only	Number of successfully validated requests for the API specification.
apispecsuccessfullyvalidatedrate	<Double>	Read-only	Rate (/s) counter for apispecsuccessfullyvalidated
apispecunmatched	<Double>	Read-only	Number of requests non matching this API specification.
apispecunmatchedrate	<Double>	Read-only	Rate (/s) counter for apispecunmatched

Operations

(click to see Properties)

- GET (ALL)
- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/apispec **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/apispec? **args=name: <String_value> ,detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get apispec resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/apispec? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "apispec": [ {

"name":<String_value>,

"apispecunmatched":<Double_value>,

"apispechitsrate":<Double_value>,

"apispechits":<Double_value>,

"apispecunmatchedrate":<Double_value>,

"apispecsuccessfullyvalidated":<Double_value>,

"apispecsuccessfullyvalidatedrate":<Double_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/stat/apispec/ name_value><String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "apispec": [ {

"name":<String_value>,

"apispecunmatched":<Double_value>,

"apispechitsrate":<Double_value>,

"apispechits":<Double_value>,

"apispecunmatchedrate":<Double_value>,

"apispecsuccessfullyvalidated":<Double_value>,

"apispecsuccessfullyvalidatedrate":<Double_value>

}]}
```

appflow

Appflow

AppFlow statistics.

NAME	DESCRIPTION
appflow	Statistics for appflow.

appflow

Statistics for appflow.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
clearstats	<String>	Read-write	Clear the statsistics / counters.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = basic, full
appflowtotaltxoctets	<Double>	Read-only	The total number of AppFlow (IPFIX) octets that the Citrix ADC has transmitted.
appflowtxoctetsrate	<Double>	Read-only	Rate (/s) counter for appflowtotaltxoctets
appflowtotalflows	<Double>	Read-only	The total number of AppFlow (IPFIX) flows that the Citrix ADC has transmitted.
appflowflowsrate	<Double>	Read-only	Rate (/s) counter for appflowtotalflows
appflowtotaltxmessagess	<Double>	Read-only	The total number of AppFlow (IPFIX) messages that the Citrix ADC has transmitted.
appflowtxmessagessrate	<Double>	Read-only	Rate (/s) counter for appflowtotaltxmessagess
appflowtotalignoctets	<Double>	Read-only	The total number of octets that the Citrix ADC has ignored for AppFlow (IPFIX).
appflowignoctetsrate	<Double>	Read-only	Rate (/s) counter for appflowtotalignoctets
appflowtotalignpacketss	<Double>	Read-only	The total number of packets that the Citrix ADC has

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			ignored for AppFlow (IPFIX).
appflowignpacketssrate	<Double>	Read-only	Rate (/s) counter for appflowtotalignpacketss
appflowtotalnotxoctets	<Double>	Read-only	The total number of AppFlow (IPFIX) octets that the Citrix ADC has not transmitted.
appflownotxoctetsrate	<Double>	Read-only	Rate (/s) counter for appflowtotalnotxoctets
appflowtotalnotxflows	<Double>	Read-only	The total number of AppFlow (IPFIX) flows that the Citrix ADC has not transmitted.
appflownotxflowsrate	<Double>	Read-only	Rate (/s) counter for appflowtotalnotxflows
appflowtotalnotxpackets	<Double>	Read-only	The total number of AppFlow (IPFIX) packets that the Citrix ADC has not transmitted.
appflownotxpacketsrate	<Double>	Read-only	Rate (/s) counter for appflowtotalnotxpackets

Operations

(click to see Properties)

- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/appflow **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/appflow? **args=detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get appflow resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/appflow? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appflow": [ {

"appflowflowsrate":<Double_value>,

"appflownotxflowsrate":<Double_value>,

"appflownotxpacketsrate":<Double_value>,

"appflownotxoctetsrate":<Double_value>,

"appflowtotaltxmessagess":<Double_value>,

"appflowtxoctetsrate":<Double_value>,

"appflowtotalignoctets":<Double_value>,

"appflowtotalnotxoctets":<Double_value>,

"appflowtxmessagessrate":<Double_value>,

"appflowtotalnotxflows":<Double_value>,

"appflowtotalnotxpackets":<Double_value>,

"appflowtotalignpacketss":<Double_value>,

"appflowignoctetsrate":<Double_value>,

"appflowtotaltxoctets":<Double_value>,
```

```
"appflowignpacketssrate":<Double_value>,

"appflowtotalflows":<Double_value>

}]}
```

appfw

Application Firewall

Application Firewall statistics.

NAME	DESCRIPTION
appfw	Statistics for appfw.
appfwpolicy	Statistics for application firewall policy resource.
appfwpolicylabel	Statistics for application firewall policy label resource.
appfwprofile	Statistics for application firewall profile resource.

appfw

Statistics for appfw.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
clearstats	<String>	Read-write	Clear the statsistics / counters.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = basic, full
appfirewalltotallog	<Double>	Read-only	Total number of security check log messages generated by the Application Firewall.
appfirewalllograte	<Double>	Read-only	Rate (/s) counter for appfirewalltotallog
appfirewalltotalviol	<Double>	Read-only	Total number of security check violations seen by the Application Firewall.
appfirewallviolrate	<Double>	Read-only	Rate (/s) counter for appfirewalltotalviol
appfirewallshortavgresptime	<Double>	Read-only	Average backend response time in milliseconds over the last 7 seconds
appfirewalllongavgresptime	<Double>	Read-only	Average backend response time in milliseconds since reboot
appfirewallrequests	<Double>	Read-only	HTTP/HTTPS requests sent to your protected web servers via the Application Firewall.
appfirewallrequestsrate	<Double>	Read-only	Rate (/s) counter for appfirewallrequests

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
appfirewallreqbytes	<Double>	Read-only	Number of bytes transfered for requests
appfirewallreqbytesrate	<Double>	Read-only	Rate (/s) counter for appfirewallreqbytes
appfirewallresponses	<Double>	Read-only	HTTP/HTTPS responses sent by your protected web servers via the Application Firewall.
appfirewallresponsesrate	<Double>	Read-only	Rate (/s) counter for appfirewallresponses
appfirewallresbytes	<Double>	Read-only	Number of bytes transfered for responses
appfirewallresbytesrate	<Double>	Read-only	Rate (/s) counter for appfirewallresbytes
appfirewallaborts	<Double>	Read-only	Incomplete HTTP/HTTPS requests aborted by the client before the Application Firewall could finish processing them.
appfirewallabortsrate	<Double>	Read-only	Rate (/s) counter for appfirewallaborts
appfirewallredirects	<Double>	Read-only	HTTP/HTTPS requests redirected by the Application Firewall to a different Web page or web server. (HTTP 302)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
appfirewallredirectsrate	<Double>	Read-only	Rate (/s) counter for appfirewallredirects
appfirewalltrapsdropped	<Double>	Read-only	AppFirewall SNMP traps dropped due to time limit.
appfirewalldhtcurses s	<Double>	Read-only	Number of current appfw DHT Sessions.
appfirewalldhtcurses srate	<Double>	Read-only	Rate (/s) counter for appfirewalldhtcurses s
appfirewalldhtmaxse ss	<Double>	Read-only	Maximum of current appfw DHT sessions across all packet engines.
appfirewalldhtmaxse ssrate	<Double>	Read-only	Rate (/s) counter for appfirewalldhtmaxse ss
appfirewallviolstarturl	<Double>	Read-only	Number of Start URL security check violations seen by the Application Firewall.
appfirewallviolstarturl rate	<Double>	Read-only	Rate (/s) counter for appfirewallviolstarturl
appfirewallvioldenyur l	<Double>	Read-only	Number of Deny URL security check violations seen by the Application Firewall.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
appfirewallvioldenyurlrate	<Double>	Read-only	Rate (/s) counter for appfirewallvioldenyurl
appfirewallviolreferer header	<Double>	Read-only	Number of Referer Header security check violations seen by the Application Firewall.
appfirewallviolreferer headerrate	<Double>	Read-only	Rate (/s) counter for appfirewallviolreferer header
appfirewallviolbuffero verflow	<Double>	Read-only	Number of Buffer Overflow security check violations seen by the Application Firewall.
appfirewallviolbuffero verflowrate	<Double>	Read-only	Rate (/s) counter for appfirewallviolbuffero verflow
appfirewallviolgrpc	<Double>	Read-only	Number of gRPC security check violations seen by the Application Firewall.
appfirewallviolgrpcrate	<Double>	Read-only	Rate (/s) counter for appfirewallviolgrpc
appfirewallpostbodylimitviolations	<Double>	Read-only	Number of Post Body Limit security check violations seen by the Application Firewall.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
appfirewallpostbodylimitviolationsrate	<Double>	Read-only	Rate (/s) counter for appfirewallpostbodylimitviolations
appfirewallviolcookie	<Double>	Read-only	Number of Cookie Consistency security check violations seen by the Application Firewall.
appfirewallviolcookierate	<Double>	Read-only	Rate (/s) counter for appfirewallviolcookie
appfirewallviolcookiehijack	<Double>	Read-only	Number of Cookie Hijacking security violations seen by the Application Firewall.
appfirewallviolcookiehijackrate	<Double>	Read-only	Rate (/s) counter for appfirewallviolcookiehijack
appfirewallviolcsrftag	<Double>	Read-only	Number of Cross Site Request Forgery form tag security check violations seen by the Application Firewall.
appfirewallviolcsrftagrate	<Double>	Read-only	Rate (/s) counter for appfirewallviolcsrftag
appfirewallviolxss	<Double>	Read-only	Number of HTML Cross-Site Scripting security check violations seen by the Application Firewall.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
appfirewallviolxssrate	<Double>	Read-only	Rate (/s) counter for appfirewallviolxss
appfirewallviolsql	<Double>	Read-only	Number of HTML SQL Injection security check violations seen by the Application Firewall.
appfirewallviolsqlrate	<Double>	Read-only	Rate (/s) counter for appfirewallviolsql
appfirewallviolfieldformat	<Double>	Read-only	Number of Field Format security check violations seen by the Application Firewall.
appfirewallviolfieldformatrate	<Double>	Read-only	Rate (/s) counter for appfirewallviolfieldformat
appfirewallviolfieldconsistency	<Double>	Read-only	Number of Field Consistency security check violations seen by the Application Firewall.
appfirewallviolfieldconsistencyrate	<Double>	Read-only	Rate (/s) counter for appfirewallviolfieldconsistency
appfirewallviolfileuploadtypes	<Double>	Read-only	Number of Field Upload Types security check violations seen by the Application Firewall.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
appfirewallviolfileuploadtypesrate	<Double>	Read-only	Rate (/s) counter for appfirewallviolfileuploadtypes
appfirewallviolxmlpayloadcontenttypemismatch	<Double>	Read-only	Number of Mismatched Content-Type in request with XML Payload security check violations seen by the Application Firewall.
appfirewallviolxmlpayloadcontenttypemismatchrate	<Double>	Read-only	Rate (/s) counter for appfirewallviolxmlpayloadcontenttypemismatch
appfirewallviolcreditcard	<Double>	Read-only	Number of Credit Card security check violations seen by the Application Firewall.
appfirewallviolcreditcardrate	<Double>	Read-only	Rate (/s) counter for appfirewallviolcreditcard
appfirewallviolsafeobject	<Double>	Read-only	Number of Safe Object security check violations seen by the Application Firewall.
appfirewallviolsafeobjectrate	<Double>	Read-only	Rate (/s) counter for appfirewallviolsafeobject
appfirewallviolsignature	<Double>	Read-only	Number of Signature violations seen by

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			the Application Firewall.
appfirewallviolsignaturerate	<Double>	Read-only	Rate (/s) counter for appfirewallviolsignature
appfirewallviolcontenttype	<Double>	Read-only	Number of Content type security check violations seen by the Application Firewall.
appfirewallviolcontenttyperate	<Double>	Read-only	Rate (/s) counter for appfirewallviolcontenttype
appfirewallviolcmd	<Double>	Read-only	Number of HTML CMD Injection security check violations seen by the Application Firewall.
appfirewallviolcmdrate	<Double>	Read-only	Rate (/s) counter for appfirewallviolcmd
appfirewallvioljsondos	<Double>	Read-only	Number of JSON Denial-of-Service security check violations seen by the Application Firewall.
appfirewallvioljsondosrate	<Double>	Read-only	Rate (/s) counter for appfirewallvioljsondos
appfirewallvioljsonsql	<Double>	Read-only	Number of JSON SQL Injection security check violations seen by

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			the Application Firewall.
appfirewallvioljsonsqlrate	<Double>	Read-only	Rate (/s) counter for appfirewallvioljsonsql
appfirewallvioljsonxss	<Double>	Read-only	Number of JSON Cross-Site Scripting (XSS) security check violations seen by the Application Firewall.
appfirewallvioljsonxssrate	<Double>	Read-only	Rate (/s) counter for appfirewallvioljsonxss
appfirewallvioljsoncmd	<Double>	Read-only	Number of JSON Command Injection security check violations seen by the Application Firewall.
appfirewallvioljsoncmdrate	<Double>	Read-only	Rate (/s) counter for appfirewallvioljsoncmd
appfirewallviolwellformednessviolations	<Double>	Read-only	Number of XML Format security check violations seen by the Application Firewall.
appfirewallviolwellformednessviolationsrate	<Double>	Read-only	Rate (/s) counter for appfirewallviolwellformednessviolations
appfirewallviolxdosviolations	<Double>	Read-only	Number of XML Denial-of-Service security check violations seen by

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			the Application Firewall.
appfirewallviolxdosviolationsrate	<Double>	Read-only	Rate (/s) counter for appfirewallviolxdosviolations
appfirewallviolmsgvalviolations	<Double>	Read-only	Number of XML Message Validation security check violations seen by the Application Firewall.
appfirewallviolmsgvalviolationsrate	<Double>	Read-only	Rate (/s) counter for appfirewallviolmsgvalviolations
appfirewallviolwsiviolations	<Double>	Read-only	Number of Web Services Interoperability (WS-I) security check violations seen by the Application Firewall.
appfirewallviolwsiviolationsrate	<Double>	Read-only	Rate (/s) counter for appfirewallviolwsiviolations
appfirewallviolxmlsqlviolations	<Double>	Read-only	Number of XML SQL Injection security check violations seen by the Application Firewall.
appfirewallviolxmlsqlviolationsrate	<Double>	Read-only	Rate (/s) counter for appfirewallviolxmlsqlviolations

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
appfirewallviolxmlxssviolations	<Double>	Read-only	Number of XML Cross-Site Scripting (XSS) security check violations seen by the Application Firewall.
appfirewallviolxmlxssviolationsrate	<Double>	Read-only	Rate (/s) counter for appfirewallviolxmlxssviolations
appfirewallviolxmlattachmentviolations	<Double>	Read-only	Number of XML Attachment security check violations seen by the Application Firewall.
appfirewallviolxmlattachmentviolationsrate	<Double>	Read-only	Rate (/s) counter for appfirewallviolxmlattachmentviolations
appfirewallviolxmlsoapfaultviolations	<Double>	Read-only	Number of requests returning soap:fault from the backend server
appfirewallviolxmlsoapfaultviolationsrate	<Double>	Read-only	Rate (/s) counter for appfirewallviolxmlsoapfaultviolations
appfirewallviolxmlgenviolations	<Double>	Read-only	Number of requests returning XML generic error from the backend server
appfirewallviolxmlgenviolationsrate	<Double>	Read-only	Rate (/s) counter for appfirewallviolxmlgenviolations
appfirewallviolsqlgram	<Double>	Read-only	Number of HTML SQL Injection

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			security check violations (using SQL grammar) seen by the Application Firewall.
appfirewallviolsqlgramrate	<Double>	Read-only	Rate (/s) counter for appfirewallviolsqlgram
appfirewallvioljsonsqlgram	<Double>	Read-only	Number of JSON SQL Injection security check violations (reported using SQL grammar) seen by the Application Firewall.
appfirewallvioljsonsqlgramrate	<Double>	Read-only	Rate (/s) counter for appfirewallvioljsonsqlgram
appfirewallviolsqlcombined	<Double>	Read-only	Number of combined SQL Injection security check violations seen by the Application Firewall.
appfirewallviolsqlcombinedrate	<Double>	Read-only	Rate (/s) counter for appfirewallviolsqlcombined
appfirewallviolxxecombined	<Double>	Read-only	Number of combined XXE security check violations seen by the Application Firewall.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
appfirewallviolxxecombinedrate	<Double>	Read-only	Rate (/s) counter for appfirewallviolxxecombined
appfirewallviolxsscombined	<Double>	Read-only	Number of combined Cross-Site Scripting security check violations seen by the Application Firewall.
appfirewallviolxsscombinedrate	<Double>	Read-only	Rate (/s) counter for appfirewallviolxsscombined
appfirewallviolowaspcombined	<Double>	Read-only	Number of combined OWASP security check violations seen by the Application Firewall.
appfirewallviolowaspcombinedrate	<Double>	Read-only	Rate (/s) counter for appfirewallviolowaspcombined
appfirewallviolcmdgram	<Double>	Read-only	Number of HTML CMD Injection security check violations (using SQL grammar) seen by the Application Firewall.
appfirewallviolcmdgramrate	<Double>	Read-only	Rate (/s) counter for appfirewallviolcmdgram
appfirewallvioljsoncmdgram	<Double>	Read-only	Number of JSON CMD Injection security check violations (reported

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			using CMD grammar) seen by the Application Firewall.
appfirewallvioljsoncmdgramrate	<Double>	Read-only	Rate (/s) counter for appfirewallvioljsoncmdgram
appfirewallviolblockkeyword	<Double>	Read-only	Number of Block Keyword security check violations seen by the Application Firewall.
appfirewallviolblockkeywordrate	<Double>	Read-only	Rate (/s) counter for appfirewallviolblockkeyword
appfirewallvioljsonblockkeyword	<Double>	Read-only	Number of JSON Block Keyword security check violations seen by the Application Firewall.
appfirewallvioljsonblockkeywordrate	<Double>	Read-only	Rate (/s) counter for appfirewallvioljsonblockkeyword
appfirewalllogstarturl	<Double>	Read-only	Number of Start URL security check log messages generated by the Application Firewall.
appfirewalllogstarturlrate	<Double>	Read-only	Rate (/s) counter for appfirewalllogstarturl
appfirewalllogdenyurl	<Double>	Read-only	Number of Deny URL security check log messages

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			generated by the Application Firewall.
appfirewalllogdenyurlrate	<Double>	Read-only	Rate (/s) counter for appfirewalllogdenyurl
appfirewalllogreferer header	<Double>	Read-only	Number of Referer Header security check log messages generated by the Application Firewall.
appfirewalllogreferer headerrate	<Double>	Read-only	Rate (/s) counter for appfirewalllogreferer header
appfirewalllogbuffero verflow	<Double>	Read-only	Number of Buffer Overflow security check log messages generated by the Application Firewall.
appfirewalllogbuffero verflowrate	<Double>	Read-only	Rate (/s) counter for appfirewalllogbuffero verflow
appfirewallgrpclogs	<Double>	Read-only	Number of gRPC security check logs seen by the Application Firewall.
appfirewallgrpclogsra te	<Double>	Read-only	Rate (/s) counter for appfirewallgrpclogs
appfirewallpostbodyli mitlogs	<Double>	Read-only	Number of Post Body Limit security check logs seen by the Application Firewall.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
appfirewallpostbodylimitlogsrate	<Double>	Read-only	Rate (/s) counter for appfirewallpostbodylimitlogs
appfirewalllogcookie	<Double>	Read-only	Number of Cookie Consistency security check log messages generated by the Application Firewall.
appfirewalllogcookierate	<Double>	Read-only	Rate (/s) counter for appfirewalllogcookie
appfirewalllogcookiehijack	<Double>	Read-only	Number of Cookie Hijacking security violation log messages generated by the Application Firewall.
appfirewalllogcookiehijackrate	<Double>	Read-only	Rate (/s) counter for appfirewalllogcookiehijack
appfirewalllogcsrftag	<Double>	Read-only	Number of Cross Site Request Forgery form tag security check log messages generated by the Application Firewall.
appfirewalllogcsrftagrate	<Double>	Read-only	Rate (/s) counter for appfirewalllogcsrftag
appfirewalllogxss	<Double>	Read-only	Number of HTML Cross-Site Scripting security check log messages generated by the Application Firewall.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
appfirewalllogxssrate	<Double>	Read-only	Rate (/s) counter for appfirewalllogxss
appfirewalllogtransformxss	<Double>	Read-only	Number of HTML Cross-Site Scripting security check transform log messages generated by the Application Firewall.
appfirewalllogtransformxssrate	<Double>	Read-only	Rate (/s) counter for appfirewalllogtransformxss
appfirewalllogsql	<Double>	Read-only	Number of HTML SQL Injection security check log messages generated by the Application Firewall.
appfirewalllogsqlrate	<Double>	Read-only	Rate (/s) counter for appfirewalllogsql
appfirewalllogtransformsql	<Double>	Read-only	Number of HTML SQL Injection security check transform log messages generated by the Application Firewall.
appfirewalllogtransformsqlrate	<Double>	Read-only	Rate (/s) counter for appfirewalllogtransformsql
appfirewalllogfieldformat	<Double>	Read-only	Number of Field Format security check log messages

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			generated by the Application Firewall.
appfirewalllogfieldformatrate	<Double>	Read-only	Rate (/s) counter for appfirewalllogfieldformat
appfirewalllogfieldconsistency	<Double>	Read-only	Number of Field Consistency security check log messages generated by the Application Firewall.
appfirewalllogfieldconsistencyrate	<Double>	Read-only	Rate (/s) counter for appfirewalllogfieldconsistency
appfirewalllogcreditcard	<Double>	Read-only	Number of Credit Card security check log messages generated by the Application Firewall.
appfirewalllogcreditcardrate	<Double>	Read-only	Rate (/s) counter for appfirewalllogcreditcard
appfirewalllogsafeobject	<Double>	Read-only	Number of Safe Object security check log messages generated by the Application Firewall.
appfirewalllogsafeobjectrate	<Double>	Read-only	Rate (/s) counter for appfirewalllogsafeobject
appfirewallsignaturelogs	<Double>	Read-only	Number of Signature logs generated by the Application Firewall.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
appfirewallsignaturelogsrate	<Double>	Read-only	Rate (/s) counter for appfirewallsignaturelogs
appfirewalllogcontenttype	<Double>	Read-only	Number of content type security check log messages generated by the Application Firewall.
appfirewalllogcontenttyperate	<Double>	Read-only	Rate (/s) counter for appfirewalllogcontenttype
appfirewalllogsjsondos	<Double>	Read-only	Number of JSON Denial-of-Service security check log messages generated by the Application Firewall.
appfirewalllogsjsondosrate	<Double>	Read-only	Rate (/s) counter for appfirewalllogsjsondos
appfirewalllogsjsonsql	<Double>	Read-only	Number of JSON SQL Injection security check log messages generated by the Application Firewall.
appfirewalllogsjsonsqlrate	<Double>	Read-only	Rate (/s) counter for appfirewalllogsjsonsql
appfirewalllogsjsonxss	<Double>	Read-only	Number of JSON Cross-Site Scripting (XSS) security check log messages

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			generated by the Application Firewall.
appfirewalllogsjsonxsrate	<Double>	Read-only	Rate (/s) counter for appfirewalllogsjsonxss
appfirewalllogsjsoncmd	<Double>	Read-only	Number of JSON Command Injection security check log messages generated by the Application Firewall.
appfirewalllogsjsoncmdrate	<Double>	Read-only	Rate (/s) counter for appfirewalllogsjsoncmd
appfirewalllogfileuploadtypes	<Double>	Read-only	Number of File Upload Types security check log messages generated by the Application Firewall.
appfirewalllogfileuploadtypesrate	<Double>	Read-only	Rate (/s) counter for appfirewalllogfileuploadtypes
appfirewalllogxmlpayloadcontenttypemismatch	<Double>	Read-only	Number of Mismatched Content-Type in request with XML Payload security check logs seen by the Application Firewall.
appfirewalllogxmlpayloadcontenttypemismatchrate	<Double>	Read-only	Rate (/s) counter for appfirewalllogxmlpay

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			loadcontenttypemismatch
appfirewalllogcmd	<Double>	Read-only	Number of HTML Command Injection security check log messages generated by the Application Firewall.
appfirewalllogcmdrate	<Double>	Read-only	Rate (/s) counter for appfirewalllogcmd
appfirewallwellformednesslogs	<Double>	Read-only	Number of XML Format security check log messages generated by the Application Firewall.
appfirewallwellformednesslogsrate	<Double>	Read-only	Rate (/s) counter for appfirewallwellformednesslogs
appfirewallxdoslogs	<Double>	Read-only	Number of XML Denial-of-Service security check log messages generated by the Application Firewall.
appfirewallxdoslogsrate	<Double>	Read-only	Rate (/s) counter for appfirewallxdoslogs
appfirewallmsgvallogs	<Double>	Read-only	Number of XML Message Validation security check log messages generated by the Application Firewall.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
appfirewallmsgvallogsrate	<Double>	Read-only	Rate (/s) counter for appfirewallmsgvallogs
appfirewallwsilogs	<Double>	Read-only	Number of Web Services Interoperability (WS-I) security check log messages generated by the Application Firewall.
appfirewallwsilogsrate	<Double>	Read-only	Rate (/s) counter for appfirewallwsilogs
appfirewallxmlsqllogs	<Double>	Read-only	Number of XML SQL Injection security check log messages generated by the Application Firewall.
appfirewallxmlsqllogsrate	<Double>	Read-only	Rate (/s) counter for appfirewallxmlsqllogs
appfirewallxmlxsslogs	<Double>	Read-only	Number of XML Cross-Site Scripting (XSS) security check log messages generated by the Application Firewall.
appfirewallxmlxsslogsrate	<Double>	Read-only	Rate (/s) counter for appfirewallxmlxsslogs
appfirewallxmlattachmentlogs	<Double>	Read-only	Number of XML Attachment security check log messages generated by the Application Firewall.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
appfirewallxmlattachmentlogsrate	<Double>	Read-only	Rate (/s) counter for appfirewallxmlattachmentlogs
appfirewallxmlsoapfaultlogs	<Double>	Read-only	Number of requests generating soap:fault log messages
appfirewallxmlsoapfaultlogsrate	<Double>	Read-only	Rate (/s) counter for appfirewallxmlsoapfaultlogs
appfirewallxmlgenlogs	<Double>	Read-only	Number of requests generating XML generic error log messages
appfirewallxmlgenlogsrate	<Double>	Read-only	Rate (/s) counter for appfirewallxmlgenlogs
appfirewalllogsqlgram	<Double>	Read-only	Number of HTML SQL Injection security check log messages (reported by SQL grammar) generated by the Application Firewall.
appfirewalllogsqlgramrate	<Double>	Read-only	Rate (/s) counter for appfirewalllogsqlgram
appfirewalllogsjsonsqlgram	<Double>	Read-only	Number of JSON SQL Injection security check log messages (reported by SQL grammar) generated by the Application Firewall.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
appfirewalllogsjsonsqlgramrate	<Double>	Read-only	Rate (/s) counter for appfirewalllogsjsonsqlgram
appfirewalllogcmdgram	<Double>	Read-only	Number of HTML CMD Injection security check log messages (reported by CMD grammar) generated by the Application Firewall.
appfirewalllogcmdgramrate	<Double>	Read-only	Rate (/s) counter for appfirewalllogcmdgram
appfirewalllogsjsoncmdgram	<Double>	Read-only	Number of JSON CMD Injection security check log messages (reported by CMD grammar) generated by the Application Firewall.
appfirewalllogsjsoncmdgramrate	<Double>	Read-only	Rate (/s) counter for appfirewalllogsjsoncmdgram
appfirewalllogblockkeyword	<Double>	Read-only	Number of HTML Block Keyword security check log messages generated by the Application Firewall.
appfirewalllogblockkeywordrate	<Double>	Read-only	Rate (/s) counter for appfirewalllogblockkeyword
appfirewalllogjsonblockkeyword	<Double>	Read-only	Number of JSON Block Keyword

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			security check log messages generated by the Application Firewall.
appfirewalllogjsonblockkeywordrate	<Double>	Read-only	Rate (/s) counter for appfirewalllogjsonblockkeyword
appfirewallret4xx	<Double>	Read-only	Number of requests returning HTTP 4xx from the backend server
appfirewallret4xxrate	<Double>	Read-only	Rate (/s) counter for appfirewallret4xx
appfirewallret5xx	<Double>	Read-only	Number of requests returning HTTP 5xx from the backend server
appfirewallret5xxrate	<Double>	Read-only	Rate (/s) counter for appfirewallret5xx
appfirewallcfgstarturlclosure	<Double>	Read-only	Number of profiles with Start URL Closure enabled in the Application Firewall.
appfirewallcfgcookietransforms	<Double>	Read-only	Number of profiles with Config Cookie Transforms enabled in the Application Firewall.
appfirewallcfgcrosssitescriptingtransformunsafehtml	<Double>	Read-only	Number of profiles with CrossSite Scripting Transform Unsafe HTML

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			enabled in the Application Firewall.
appfirewallcfgcrosssitescriptingcheckcompleteurls	<Double>	Read-only	Number of profiles with CrossSite Scripting Check Complete URLs enabled in the Application Firewall.
appfirewallcfgsqlinjectiongrammar	<Double>	Read-only	Number of profiles with SQL Injection Grammar enabled in the Application Firewall.
appfirewallcfgsqlinjectiontransformspecialchars	<Double>	Read-only	Number of profiles with SQL Injection Transform Special Characters enabled in the Application Firewall.
appfirewallcfgsqlinjectioncheckcsqlwildchars	<Double>	Read-only	Number of profiles with SQL Injection Check SQL Wild Characters enabled in the Application Firewall.
appfirewallcfgcreditcardxout	<Double>	Read-only	Number of profiles with Credit Card XOut enabled in the Application Firewall.
appfirewallcfgdosecurecreditcardlogging	<Double>	Read-only	Number of profiles with Do Secure Credit Card Logging enabled in the Application Firewall.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
appfirewallcfgstreaming	<Double>	Read-only	Number of profiles with Streaming enabled in the Application Firewall.
appfirewallcfgtrace	<Double>	Read-only	Number of profiles with Trace enabled in the Application Firewall.
appfirewallcfgjsonsqlinjectiongrammar	<Double>	Read-only	Number of profiles with JSON SQL Injection Grammar enabled in the Application Firewall.
appfirewallcfgxmlsqlinjectionchecksqlwildchars	<Double>	Read-only	Number of profiles with XML SQL Injection Check SQL Wild Chars enabled in the Application Firewall.
appfirewallcfgusehtmlerrorobject	<Double>	Read-only	Number of profiles with Use HTML Error Object enabled in the Application Firewall.
appfirewallcfglogeverypolicyhit	<Double>	Read-only	Number of profiles with Log Every Policy Hit enabled in the Application Firewall.
appfirewallcfgexemptclosureurlsfromsecuritychecks	<Double>	Read-only	Number of profiles with Exempt Closure URLs From Security Checks enabled in the Application Firewall.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
appfirewallcfgcanonicalizehtmlresponse	<Double>	Read-only	Number of profiles with Canonicalize HTML Response enabled in the Application Firewall.
appfirewallcfgenableformtagging	<Double>	Read-only	Number of profiles with Enable Form Tagging enabled in the Application Firewall.
appfirewallcfgsessionlessurlclosure	<Double>	Read-only	Number of profiles with Sessionless URL Closure enabled in the Application Firewall.
appfirewallcfgsemicolonfieldseparator	<Double>	Read-only	Number of profiles with Semicolon Field Separator enabled in the Application Firewall.
appfirewallcfgexcludefileuploadfromchecks	<Double>	Read-only	Number of profiles with Exclude File Upload From Checks enabled in the Application Firewall.
appfirewallcfgcheckrequestheaders	<Double>	Read-only	Number of profiles with Check Request Headers enabled in the Application Firewall.
appfirewallcfgoptimizepartialreqs	<Double>	Read-only	Number of profiles with Optimize Partial Reqs enabled in the Application Firewall.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
appfirewallcfgurldecoderequestcookies	<Double>	Read-only	Number of profiles with URL Decode Request Cookies enabled in the Application Firewall.
appfirewallcfgpercentdecoderecursively	<Double>	Read-only	Number of profiles with Percent Decode Recursively enabled in the Application Firewall.
appfirewallcfginsertcookiesamesiteattribute	<Double>	Read-only	Number of profiles with Insert Cookie SameSite Attribute enabled in the Application Firewall.
appfirewallcfgfakeaccountdetection	<Double>	Read-only	Number of profiles with Fake Account Detection enabled in the Application Firewall.
appfirewallcfgfieldscanenabled	<Double>	Read-only	Number of profiles with field scan enabled in the Application Firewall.
appfirewallcfgfieldscanenabledjson	<Double>	Read-only	Number of profiles with JSON field scan enabled in the Application Firewall.
appfirewallcfgmessagescanenabled	<Double>	Read-only	Number of profiles with message scan enabled in the Application Firewall.
appfirewallcfgmessagescanenabledjson	<Double>	Read-only	Number of profiles with JSON message

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			scan enabled in the Application Firewall.

Operations

(click to see Properties)

- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/appfw **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/appfw? **args=detail: <Boolean_value> ,fullvalues:**

<Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>

Use this query-parameter to get appfw resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/appfw? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfw": [ {

"appfirewalllogsqlgram":<Double_value>,

"appfirewalllogsjsoncmdgramrate":<Double_value>,

"appfirewallvioljsonsql":<Double_value>,

"appfirewallvioldenyurlrate":<Double_value>,

"appfirewalllogcontenttyperate":<Double_value>,

"appfirewallwsilogsrate":<Double_value>,

"appfirewallxmlsqllogs":<Double_value>,

"appfirewallviolxxecombined":<Double_value>,
```

```
"appfirewallcfgcanonicalizehtmlresponse":<Double_value>,

"appfirewallxmlgenlogsrate":<Double_value>,

"appfirewallcfgstarturlclosure":<Double_value>,

"appfirewallviolxmlgenviolations":<Double_value>,

"appfirewallcfgcrosssitescriptingtransformunsafehtml":<Double_value>,

"appfirewalllogsjsonsqlrate":<Double_value>,

"appfirewalllogfieldconsistencyrate":<Double_value>,

"appfirewalllogtransformsql":<Double_value>,

"appfirewallviolrate":<Double_value>,

"appfirewallvioljsonsqlgramrate":<Double_value>,

"appfirewallredirectsrate":<Double_value>,

"appfirewallret4xx":<Double_value>,

"appfirewallviolxmlgenviolationsrate":<Double_value>,

"appfirewallviolxsscombined":<Double_value>,

"appfirewallresponses":<Double_value>,

"appfirewalllogbufferoverflowrate":<Double_value>,

"appfirewalllogrefererheader":<Double_value>,

"appfirewallviolxmlsqlviolationsrate":<Double_value>,

"appfirewallredirects":<Double_value>,

"appfirewallgrpclogs":<Double_value>,

"appfirewallresponsesrate":<Double_value>,

"appfirewalllogfileuploadtypes":<Double_value>,
```

```
"appfirewallrequests":<Double_value>,

"appfirewallcfgmessagescanenabled":<Double_value>,

"appfirewalllogxss":<Double_value>,

"appfirewallviolcontenttyperate":<Double_value>,

"appfirewallvioldenyurl":<Double_value>,

"appfirewallcfgfieldscanenabled":<Double_value>,

"appfirewallxmlsoapfaultlogsrate":<Double_value>,

"appfirewallcfgdosecurecreditcardlogging":<Double_value>,

"appfirewallret5xx":<Double_value>,

"appfirewallviolcsrftagrate":<Double_value>,

"appfirewallpostbodylimitlogs":<Double_value>,

"appfirewallsignaturelogsrate":<Double_value>,

"appfirewallvioljsondos":<Double_value>,

"appfirewallcfglogeverypolicyhit":<Double_value>,

"appfirewallviolxmlsoapfaultviolationsrate":<Double_value>,

"appfirewallviolxdosviolationsrate":<Double_value>,

"appfirewallviolxss":<Double_value>,

"appfirewalllogxmlpayloadcontenttypemismatchrate":<Double_value>,

"appfirewallcfgstreaming":<Double_value>,

"appfirewalllogsjsonxssrate":<Double_value>,

"appfirewallxmlattachmentlogs":<Double_value>,

"appfirewallpostbodylimitviolations":<Double_value>,
```

```
"appfirewallviolcookie":<Double_value>,

"appfirewallviolsafeobject":<Double_value>,

"appfirewallxmlgenlogs":<Double_value>,

"appfirewallviolsqlcombined":<Double_value>,

"appfirewallviolwellformednessviolations":<Double_value>,

"appfirewallviolsqlcombinedrate":<Double_value>,

"appfirewallviolxmlsqlviolations":<Double_value>,

"appfirewalllogstarturlrate":<Double_value>,

"appfirewalllogsjsonsql":<Double_value>,

"appfirewallviolsqlgramrate":<Double_value>,

"appfirewallpostbodylimitviolationsrate":<Double_value>,

"appfirewallviolxmlpayloadcontenttypemismatch":<Double_value>,

"appfirewallret4xxrate":<Double_value>,

"appfirewalllogcsrftag":<Double_value>,

"appfirewallviolblockkeywordrate":<Double_value>,

"appfirewallcfgsessionlessurlclosure":<Double_value>,

"appfirewallxdoslogsrate":<Double_value>,

"appfirewalllogsafeobjectrate":<Double_value>,

"appfirewallcfgsemicolonfieldseparator":<Double_value>,

"appfirewallwellformednesslogsrate":<Double_value>,

"appfirewallreqbytes":<Double_value>,

"appfirewallcfgfieldscanenabledjson":<Double_value>,
```

```
"appfirewallvioljsonblockkeywordrate":<Double_value>,

"appfirewalllogjsonblockkeywordrate":<Double_value>,

"appfirewalllogdenyurl":<Double_value>,

"appfirewallviolrefererheaderrate":<Double_value>,

"appfirewallviolrefererheader":<Double_value>,

"appfirewalllogstarturl":<Double_value>,

"appfirewallret5xxrate":<Double_value>,

"appfirewallviolcmdgramrate":<Double_value>,

"appfirewalllogfileuploadtypesrate":<Double_value>,

"appfirewallviolcreditcardrate":<Double_value>,

"appfirewalltotallog":<Double_value>,

"appfirewalllogcmdgram":<Double_value>,

"appfirewallviolmsgvalviolationsrate":<Double_value>,

"appfirewallviolcmdgram":<Double_value>,

"appfirewallviolgrpcrate":<Double_value>,

"appfirewallviolcookiehijackrate":<Double_value>,

"appfirewallresbytes":<Double_value>,

"appfirewalllogcontenttype":<Double_value>,

"appfirewallvioljsonsqlrate":<Double_value>,

"appfirewallcfgenableformtagging":<Double_value>,

"appfirewallviolcmd":<Double_value>,

"appfirewallcfginsertcookiesamesiteattribute":<Double_value>,
```

```
"appfirewallcfgsqlinjectiongrammar":<Double_value>,

"appfirewallcfgexemptclosureurlsfromsecuritychecks":<Double_value>,

"appfirewallmsgvallogs":<Double_value>,

"appfirewalllogsjsonsqlgram":<Double_value>,

"appfirewalllogtransformxss":<Double_value>,

"appfirewalltrapsdropped":<Double_value>,

"appfirewalllogsjsonsqlgramrate":<Double_value>,

"appfirewalllogxssrate":<Double_value>,

"appfirewallpostbodylimitlogsrate":<Double_value>,

"appfirewallviolwellformednessviolationsrate":<Double_value>,

"appfirewallviolsqlrate":<Double_value>,

"appfirewalllogsjsondos":<Double_value>,

"appfirewallwellformednesslogs":<Double_value>,

"appfirewallviolcookierate":<Double_value>,

"appfirewallcfgurldecoderequestcookies":<Double_value>,

"appfirewallviolbufferoverflowrate":<Double_value>,

"appfirewalllogsjsonxss":<Double_value>,

"appfirewallvioljsonxssrate":<Double_value>,

"appfirewalllogbufferoverflow":<Double_value>,

"appfirewallviolfieldformat":<Double_value>,

"appfirewalllogfieldformatrate":<Double_value>,

"appfirewallviolwsiviolationsrate":<Double_value>,
```

```
"appfirewalllogtransformxssrate":<Double_value>,

"appfirewallviolsignaturerate":<Double_value>,

"appfirewalllogsjsoncmdgram":<Double_value>,

"appfirewalllogfieldformat":<Double_value>,

"appfirewalllogjsonblockkeyword":<Double_value>,

"appfirewallwsilogs":<Double_value>,

"appfirewallreqbytesrate":<Double_value>,

"appfirewalldhtmaxsess":<Double_value>,

"appfirewallviolbufferoverflow":<Double_value>,

"appfirewallxdoslogs":<Double_value>,

"appfirewallxmlxsslogsrate":<Double_value>,

"appfirewallaborts":<Double_value>,

"appfirewallviolxxecombinedrate":<Double_value>,

"appfirewallviolxmlattachmentviolationsrate":<Double_value>,

"appfirewalldhtcursess":<Double_value>,

"appfirewalllogxmlpayloadcontenttypemismatch":<Double_value>,

"appfirewallcfgfakeaccountdetection":<Double_value>,

"appfirewallmsgvallogsrate":<Double_value>,

"appfirewallxmlsqllogsrate":<Double_value>,

"appfirewalllogcmd":<Double_value>,

"appfirewalllogsjsoncmd":<Double_value>,

"appfirewallviolfieldconsistencyrate":<Double_value>,
```

```
"appfirewalllogsqlrate":<Double_value>,

"appfirewalllogblockkeywordrate":<Double_value>,

"appfirewallviolfieldformatrate":<Double_value>,

"appfirewallxmlsoapfaultlogs":<Double_value>,

"appfirewallviolxmlxssviolationsrate":<Double_value>,

"appfirewallviolfileuploadtypesrate":<Double_value>,

"appfirewallviolxmlpayloadcontenttypemismatchrate":<Double_value>,

"appfirewallviolsignature":<Double_value>,

"appfirewalllogtransformsqlrate":<Double_value>,

"appfirewallviolcreditcard":<Double_value>,

"appfirewallviolcontenttype":<Double_value>,

"appfirewallviolxssrate":<Double_value>,

"appfirewallviolxmlsoapfaultviolations":<Double_value>,

"appfirewallresbytesrate":<Double_value>,

"appfirewallviolgrpc":<Double_value>,

"appfirewallviolsafeobjectrate":<Double_value>,

"appfirewallshortavgresptime":<Double_value>,

"appfirewallsignaturelogs":<Double_value>,

"appfirewalllogsjsondosrate":<Double_value>,

"appfirewallviolmsgvalviolations":<Double_value>,

"appfirewalldhtcursessrate":<Double_value>,

"appfirewalltotalviol":<Double_value>,
```

```
"appfirewallvioljsonblockkeyword":<Double_value>,

"appfirewallvioljsoncmdgram":<Double_value>,

"appfirewallabortsrate":<Double_value>,

"appfirewallcfgusehtmlerrorobject":<Double_value>,

"appfirewallvioljsondosrate":<Double_value>,

"appfirewallxmlattachmentlogsrate":<Double_value>,

"appfirewallviolstarturl":<Double_value>,

"appfirewallcfgtrace":<Double_value>,

"appfirewallcfgcrosssitescriptingcheckcompleteurls":<Double_value>,

"appfirewallviolcookiehijack":<Double_value>,

"appfirewallviolcsrftag":<Double_value>,

"appfirewallvioljsonxss":<Double_value>,

"appfirewalllogcmdrate":<Double_value>,

"appfirewallviolxdosviolations":<Double_value>,

"appfirewalllogsjsoncmdrate":<Double_value>,

"appfirewallcfgcheckrequestheaders":<Double_value>,

"appfirewalllogsafeobject":<Double_value>,

"appfirewallvioljsoncmd":<Double_value>,

"appfirewalllogcookierate":<Double_value>,

"appfirewalllogfieldconsistency":<Double_value>,

"appfirewallxmlxsslogs":<Double_value>,

"appfirewallcfgmessagescanenabledjson":<Double_value>,
```

```
"appfirewalllogcmdgramrate":<Double_value>,

"appfirewallcfgpercentdecoderecursively":<Double_value>,

"appfirewallcfgcreditcardxout":<Double_value>,

"appfirewalllogrefererheaderrate":<Double_value>,

"appfirewallviolowaspcombined":<Double_value>,

"appfirewalllongavgresptime":<Double_value>,

"appfirewalllogdenyurlrate":<Double_value>,

"appfirewallcfgoptimizepartialreqs":<Double_value>,

"appfirewallviolxsscombinedrate":<Double_value>,

"appfirewalllogsqlgramrate":<Double_value>,

"appfirewallviolfileuploadtypes":<Double_value>,

"appfirewallcfgsqlinjectionchecksqlwildchars":<Double_value>,

"appfirewallviolxmlxssviolations":<Double_value>,

"appfirewallviolblockkeyword":<Double_value>,

"appfirewallvioljsonsqlgram":<Double_value>,

"appfirewalllogblockkeyword":<Double_value>,

"appfirewallviolsqlgram":<Double_value>,

"appfirewalldhtmaxsessrate":<Double_value>,

"appfirewalllogcreditcardrate":<Double_value>,

"appfirewallcfgjsonsqlinjectiongrammar":<Double_value>,

"appfirewalllogcookie":<Double_value>,

"appfirewallcfgcookietransforms":<Double_value>,
```

```
"appfirewalllogcookiehijackrate":<Double_value>,

"appfirewallvioljsoncmdgramrate":<Double_value>,

"appfirewalllograte":<Double_value>,

"appfirewallviolxmlattachmentviolations":<Double_value>,

"appfirewallviolsql":<Double_value>,

"appfirewalllogsql":<Double_value>,

"appfirewallvioljsoncmdrate":<Double_value>,

"appfirewallviolstarturlrate":<Double_value>,

"appfirewallrequestsrate":<Double_value>,

"appfirewallviolcmdrate":<Double_value>,

"appfirewallcfgsqlinjectiontransformspecialchars":<Double_value>,

"appfirewalllogcsrftagrate":<Double_value>,

"appfirewallviolowaspcombinedrate":<Double_value>,

"appfirewallviolfieldconsistency":<Double_value>,

"appfirewallgrpclogsrate":<Double_value>,

"appfirewalllogcreditcard":<Double_value>,

"appfirewallcfgxmlsqlinjectionchecksqlwildchars":<Double_value>,

"appfirewallviolwsiviolations":<Double_value>,

"appfirewalllogcookiehijack":<Double_value>,

"appfirewallcfgexcludefileuploadfromchecks":<Double_value>

}]}
```

appfwpolicy

Statistics for application firewall policy resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the application firewall policy. Minimum length = 1
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full
pipolicyhits	<Double>	Read-only	Number of hits on the policy
pipolicyhitsrate	<Double>	Read-only	Rate (/s) counter for pipolicyhits
pipolicyundefhits	<Double>	Read-only	Number of undef hits on the policy
pipolicyundefhitsrate	<Double>	Read-only	Rate (/s) counter for pipolicyundefhits

Operations

(click to see Properties)

- GET (ALL)
- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/appfwpolicy **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/appfwpolicy? **args=name: <String_value> ,detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get appfwpolicy resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/appfwpolicy? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwpolicy": [ {

"name":<String_value>,

"pipolicyundefhitsrate":<Double_value>,

"pipolicyhitsrate":<Double_value>,

"pipolicyundefhits":<Double_value>,

"pipolicyhits":<Double_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/stat/appfwpolicy/ name_value><String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwpolicy": [ {

"name":<String_value>,

"pipolicyundefhitsrate":<Double_value>,

"pipolicyhitsrate":<Double_value>,

"pipolicyundefhits":<Double_value>,

"pipolicyhits":<Double_value>

}]}
```

appfwpolicylabel

Statistics for application firewall policy label resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
labelname	<String>	Read-write	Name of the application firewall policy label. Minimum length = 1
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full
pipolicylabelhits	<Double>	Read-only	Number of times policy label was invoked.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
pipolicylabelhitsrate	<Double>	Read-only	Rate (/s) counter for pipolicylabelhits

Operations

(click to see Properties)

- GET (ALL)
- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/appfwpolicylabel **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/appfwpolicylabel? **args=labelname: <String_value> ,detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get appfwpolicylabel resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/appfwpolicylabel? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwpolicylabel": [ {

"labelname":<String_value>,

"pipolicylabelhits":<Double_value>,

"pipolicylabelhitsrate":<Double_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/stat/appfwpolicylabel/ labelname_value><String>
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwpolicylabel": [ {

"labelname":<String_value>,

"pipolicylabelhits":<Double_value>,

"pipolicylabelhitsrate":<Double_value>

}]}
```

appfwprofile

Statistics for application firewall profile resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the application firewall profile. Minimum length = 1
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full
appfirewallrequestsperprofile	<Double>	Read-only	HTTP/HTTPS requests sent to your protected web servers via the Application Firewall.
appfirewallrequestsperprofilerate	<Double>	Read-only	Rate (/s) counter for appfirewallrequestsperprofile
appfirewallreqbytesperprofile	<Double>	Read-only	Number of bytes transfered for requests
appfirewallreqbytesperprofilerate	<Double>	Read-only	Rate (/s) counter for appfirewallreqbytesperprofile
appfirewallresponsesperprofile	<Double>	Read-only	HTTP/HTTPS responses sent by your protected web servers via the Application Firewall.
appfirewallresponsesperprofilerate	<Double>	Read-only	Rate (/s) counter for appfirewallresponsesperprofile
appfirewallresbytesperprofile	<Double>	Read-only	Number of bytes transfered for responses

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
appfirewallresbytesperprofilerate	<Double>	Read-only	Rate (/s) counter for appfirewallresbytesperprofile
appfirewallabortsperprofile	<Double>	Read-only	Incomplete HTTP/HTTPS requests aborted by the client before the Application Firewall could finish processing them.
appfirewallabortsperprofilerate	<Double>	Read-only	Rate (/s) counter for appfirewallabortsperprofile
appfirewallredirectsperprofile	<Double>	Read-only	HTTP/HTTPS requests redirected by the Application Firewall to a different Web page or web server. (HTTP 302)
appfirewallredirectsperprofilerate	<Double>	Read-only	Rate (/s) counter for appfirewallredirectsperprofile
appfirewalllongavgresptimeperprofile	<Double>	Read-only	Average backend response time in milliseconds since reboot
appfirewallshortavgresptimeperprofile	<Double>	Read-only	Average backend response time in milliseconds over the last 7 seconds
appfirewallviolstarturlperprofile	<Double>	Read-only	Number of Start URL security check violations seen by

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			the Application Firewall.
appfirewallviolstarturlperprofilerate	<Double>	Read-only	Rate (/s) counter for appfirewallviolstarturlperprofile
appfirewallvioldenyurlperprofile	<Double>	Read-only	Number of Deny URL security check violations seen by the Application Firewall.
appfirewallvioldenyurlperprofilerate	<Double>	Read-only	Rate (/s) counter for appfirewallvioldenyurlperprofile
appfirewallviolrefererheaderperprofile	<Double>	Read-only	Number of Referer Header security check violations seen by the Application Firewall.
appfirewallviolrefererheaderperprofilerate	<Double>	Read-only	Rate (/s) counter for appfirewallviolrefererheaderperprofile
appfirewallviolbufferoverflowperprofile	<Double>	Read-only	Number of Buffer Overflow security check violations seen by the Application Firewall.
appfirewallviolbufferoverflowperprofilerate	<Double>	Read-only	Rate (/s) counter for appfirewallviolbufferoverflowperprofile
appfirewallpostbodylimitviolationsperprofile	<Double>	Read-only	Number of Post Body Limit security check violations

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			seen by the Application Firewall.
appfirewallpostbodylimitviolationsperprofilerate	<Double>	Read-only	Rate (/s) counter for appfirewallpostbodylimitviolationsperprofile
appfirewallviolcookieperprofile	<Double>	Read-only	Number of Cookie Consistency security check violations seen by the Application Firewall.
appfirewallviolcookieperprofilerate	<Double>	Read-only	Rate (/s) counter for appfirewallviolcookieperprofile
appfirewallviolcookiehijackperprofile	<Double>	Read-only	Number of Cookie Hijacking security violations seen by the Application Firewall.
appfirewallviolcookiehijackperprofilerate	<Double>	Read-only	Rate (/s) counter for appfirewallviolcookiehijackperprofile
appfirewallviolcsrftagperprofile	<Double>	Read-only	Number of Cross Site Request Forgery form tag security check violations seen by the Application Firewall.
appfirewallviolcsrftagperprofilerate	<Double>	Read-only	Rate (/s) counter for appfirewallviolcsrftagperprofile
appfirewallviolxssperprofile	<Double>	Read-only	Number of HTML Cross-Site Scripting security check

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			violations seen by the Application Firewall.
appfirewallviolxssperprofilerate	<Double>	Read-only	Rate (/s) counter for appfirewallviolxssperprofile
appfirewallviolsqlperprofile	<Double>	Read-only	Number of HTML SQL Injection security check violations seen by the Application Firewall.
appfirewallviolsqlperprofilerate	<Double>	Read-only	Rate (/s) counter for appfirewallviolsqlperprofile
appfirewallviolfieldformatperprofile	<Double>	Read-only	Number of Field Format security check violations seen by the Application Firewall.
appfirewallviolfieldformatperprofilerate	<Double>	Read-only	Rate (/s) counter for appfirewallviolfieldformatperprofile
appfirewallviolfieldconsistencyperprofile	<Double>	Read-only	Number of Field Consistency security check violations seen by the Application Firewall.
appfirewallviolfieldconsistencyperprofilerate	<Double>	Read-only	Rate (/s) counter for appfirewallviolfieldconsistencyperprofile
appfirewallviolcreditcardperprofile	<Double>	Read-only	Number of Credit Card security check violations seen by

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			the Application Firewall.
appfirewallviolcreditcardperprofilerate	<Double>	Read-only	Rate (/s) counter for appfirewallviolcreditcardperprofile
appfirewallviolsafeobjectperprofile	<Double>	Read-only	Number of Safe Object security check violations seen by the Application Firewall.
appfirewallviolsafeobjectperprofilerate	<Double>	Read-only	Rate (/s) counter for appfirewallviolsafeobjectperprofile
appfirewallviolsignatureperprofile	<Double>	Read-only	Number of Signature violations seen by the Application Firewall.
appfirewallviolsignatureperprofilerate	<Double>	Read-only	Rate (/s) counter for appfirewallviolsignatureperprofile
appfirewallviolcontenttypeperprofile	<Double>	Read-only	Number of Content Type security check violations seen by the Application Firewall.
appfirewallviolcontenttypeperprofilerate	<Double>	Read-only	Rate (/s) counter for appfirewallviolcontenttypeperprofile
appfirewallvioljsondosperprofile	<Double>	Read-only	Number of JSON Denial-of-Service security check violations seen by

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			the Application Firewall.
appfirewallvioljsondosperprofilerate	<Double>	Read-only	Rate (/s) counter for appfirewallvioljsondosperprofile
appfirewallvioljsonsqlperprofile	<Double>	Read-only	Number of JSON SQL Injection security check violations seen by the Application Firewall.
appfirewallvioljsonsqlperprofilerate	<Double>	Read-only	Rate (/s) counter for appfirewallvioljsonsqlperprofile
appfirewallvioljsonxssperprofile	<Double>	Read-only	Number of JSON Cross-Site Scripting (XSS) security check violations seen by the Application Firewall.
appfirewallvioljsonxssperprofilerate	<Double>	Read-only	Rate (/s) counter for appfirewallvioljsonxssperprofile
appfirewallvioljsoncmdperprofile	<Double>	Read-only	Number of JSON Command Injection security check violations seen by the Application Firewall.
appfirewallvioljsoncmdperprofilerate	<Double>	Read-only	Rate (/s) counter for appfirewallvioljsoncmdperprofile

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
appfirewallviolfileuploadtypesperprofile	<Double>	Read-only	Number of Field Upload Types security check violations seen by the Application Firewall.
appfirewallviolfileuploadtypesperprofilerate	<Double>	Read-only	Rate (/s) counter for appfirewallviolfileuploadtypesperprofile
appfirewallxmlpayloadcontenttypemismatchperprofile	<Double>	Read-only	Number of Mismatched Content-Type in request with XML Payload security check violations seen by the Application Firewall.
appfirewallxmlpayloadcontenttypemismatchperprofilerate	<Double>	Read-only	Rate (/s) counter for appfirewallxmlpayloadcontenttypemismatchperprofile
appfirewallviolcmdperprofile	<Double>	Read-only	Number of HTML Command Injection security check violations seen by the Application Firewall.
appfirewallviolcmdperprofilerate	<Double>	Read-only	Rate (/s) counter for appfirewallviolcmdperprofile
appfirewallviolwellformednessviolationsperprofile	<Double>	Read-only	Number of XML Format security check violations seen by the Application Firewall.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
appfirewallviolwellformednessviolationsperprofilerate	<Double>	Read-only	Rate (/s) counter for appfirewallviolwellformednessviolationsperprofile
appfirewallviolxdosviolationsperprofile	<Double>	Read-only	Number of XML Denial-of-Service security check violations seen by the Application Firewall.
appfirewallviolxdosviolationsperprofilerate	<Double>	Read-only	Rate (/s) counter for appfirewallviolxdosviolationsperprofile
appfirewallviolmsgvalviolationsperprofile	<Double>	Read-only	Number of XML Message Validation security check violations seen by the Application Firewall.
appfirewallviolmsgvalviolationsperprofilerate	<Double>	Read-only	Rate (/s) counter for appfirewallviolmsgvalviolationsperprofile
appfirewallviolwsiviolationsperprofile	<Double>	Read-only	Number of Web Services Interoperability (WS-I) security check violations seen by the Application Firewall.
appfirewallviolwsiviolationsperprofilerate	<Double>	Read-only	Rate (/s) counter for appfirewallviolwsiviolationsperprofile
appfirewallviolxmlsqlviolationsperprofile	<Double>	Read-only	Number of XML SQL Injection security

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			check violations seen by the Application Firewall.
appfirewallviolxmlsqlviolationsperprofilerate	<Double>	Read-only	Rate (/s) counter for appfirewallviolxmlsqlviolationsperprofile
appfirewallviolxmlxssviolationsperprofile	<Double>	Read-only	Number of XML Cross-Site Scripting (XSS) security check violations seen by the Application Firewall.
appfirewallviolxmlxssviolationsperprofilerate	<Double>	Read-only	Rate (/s) counter for appfirewallviolxmlxssviolationsperprofile
appfirewallviolxmlattachmentviolationsperprofile	<Double>	Read-only	Number of XML Attachment security check violations seen by the Application Firewall.
appfirewallviolxmlattachmentviolationsperprofilerate	<Double>	Read-only	Rate (/s) counter for appfirewallviolxmlattachmentviolationsperprofile
appfirewallviolxmlsoapfaultviolationsperprofile	<Double>	Read-only	Number of requests returning soap:fault from the backend server
appfirewallviolxmlsoapfaultviolationsperprofilerate	<Double>	Read-only	Rate (/s) counter for appfirewallviolxmlsoapfaultviolationsperprofile

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
appfirewallviolxmlgenericviolationsperprofile	<Double>	Read-only	Number of requests returning XML generic violation from the backend server
appfirewallviolxmlgenericviolationsperprofilerate	<Double>	Read-only	Rate (/s) counter for appfirewallviolxmlgenericviolationsperprofile
appfirewallviolsqlgramperprofile	<Double>	Read-only	Number of HTML SQL Injection security check violations (reported by SQL grammar) seen by the Application Firewall.
appfirewallviolsqlgramperprofilerate	<Double>	Read-only	Rate (/s) counter for appfirewallviolsqlgramperprofile
appfirewallvioljsonsqlgramperprofile	<Double>	Read-only	Number of JSON SQL Injection security check violations (reported by SQL grammar) seen by the Application Firewall.
appfirewallvioljsonsqlgramperprofilerate	<Double>	Read-only	Rate (/s) counter for appfirewallvioljsonsqlgramperprofile
appfirewallviolsqlcombinedperprofile	<Double>	Read-only	Number of Combined SQL Injection security check violations seen by the Application Firewall.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
appfirewallviolsqlcombinedperprofilerate	<Double>	Read-only	Rate (/s) counter for appfirewallviolsqlcombinedperprofile
appfirewallviolcombinedxxeperprofile	<Double>	Read-only	Number of combined XXE security check violations seen by the Application Firewall.
appfirewallviolcombinedxxeperprofilerate	<Double>	Read-only	Rate (/s) counter for appfirewallviolcombinedxxeperprofile
appfirewallviolcombinedxssperprofile	<Double>	Read-only	Number of combined Cross-Site Scripting security check violations seen by the Application Firewall.
appfirewallviolcombinedxssperprofilerate	<Double>	Read-only	Rate (/s) counter for appfirewallviolcombinedxssperprofile
appfirewallviolcombinedowaspperprofile	<Double>	Read-only	Number of combined OWASP security check violations seen by the Application Firewall.
appfirewallviolcombinedowaspperprofilerate	<Double>	Read-only	Rate (/s) counter for appfirewallviolcombinedowaspperprofile
appfirewallviolcmdgramperprofile	<Double>	Read-only	Number of HTML CMD Injection security check violations (reported by CMD grammar)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			seen by the Application Firewall.
appfirewallviolcmdgramperprofilerate	<Double>	Read-only	Rate (/s) counter for appfirewallviolcmdgramperprofile
appfirewallvioljsoncmdgramperprofile	<Double>	Read-only	Number of JSON CMD Injection security check violations (reported by CMD grammar) seen by the Application Firewall.
appfirewallvioljsoncmdgramperprofilerate	<Double>	Read-only	Rate (/s) counter for appfirewallvioljsoncmdgramperprofile
appfirewallviolblockkeywordperprofile	<Double>	Read-only	Number of HTML Block Keyword security check violations seen by the Application Firewall.
appfirewallviolblockkeywordperprofilerate	<Double>	Read-only	Rate (/s) counter for appfirewallviolblockkeywordperprofile
appfirewallvioljsonblockkeywordperprofile	<Double>	Read-only	Number of JSON Block Keyword security check violations seen by the Application Firewall.
appfirewallvioljsonblockkeywordperprofilerate	<Double>	Read-only	Rate (/s) counter for appfirewallvioljsonblockkeywordperprofile

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
appfirewalltotalviolperprofile	<Double>	Read-only	Number of violations seen by the application firewall on per profile basis
appfirewallviolperprofilerate	<Double>	Read-only	Rate (/s) counter for appfirewalltotalviolperprofile
appfirewalllogstarturlperprofile	<Double>	Read-only	Number of Start URL security check log messages generated by the Application Firewall.
appfirewalllogstarturlperprofilerate	<Double>	Read-only	Rate (/s) counter for appfirewalllogstarturlperprofile
appfirewalllogdenyurlperprofile	<Double>	Read-only	Number of Deny URL security check log messages generated by the Application Firewall.
appfirewalllogdenyurlperprofilerate	<Double>	Read-only	Rate (/s) counter for appfirewalllogdenyurlperprofile
appfirewalllogrefererheaderperprofile	<Double>	Read-only	Number of Referer Header security check log messages generated by the Application Firewall.
appfirewalllogrefererheaderperprofilerate	<Double>	Read-only	Rate (/s) counter for appfirewalllogrefererheaderperprofile
appfirewalllogbufferoverflowperprofile	<Double>	Read-only	Number of Buffer Overflow security

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			check log messages generated by the Application Firewall.
appfirewalllogbufferoverflowperprofilerate	<Double>	Read-only	Rate (/s) counter for appfirewalllogbufferoverflowperprofile
appfirewallgrpclogsperprofile	<Double>	Read-only	Number of gRPC checks seen by the Application Firewall.
appfirewallgrpclogsperprofilerate	<Double>	Read-only	Rate (/s) counter for appfirewallgrpclogsperprofile
appfirewallpostbodylimitlogsperprofile	<Double>	Read-only	Number of Post Body Limit security check logs seen by the Application Firewall.
appfirewallpostbodylimitlogsperprofilerate	<Double>	Read-only	Rate (/s) counter for appfirewallpostbodylimitlogsperprofile
appfirewalllogcookieperprofile	<Double>	Read-only	Number of Cookie Consistency security check log messages generated by the Application Firewall.
appfirewalllogcookieperprofilerate	<Double>	Read-only	Rate (/s) counter for appfirewalllogcookieperprofile
appfirewalllogcookiehijackperprofile	<Double>	Read-only	Number of Cookie Hijacking security violation log messages generated

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			by the Application Firewall.
appfirewalllogcookie hijackperprofilerate	<Double>	Read-only	Rate (/s) counter for appfirewalllogcookie hijackperprofile
appfirewalllogcsrftag perprofile	<Double>	Read-only	Number of Cross Site Request Forgery form tag security check log messages generated by the Application Firewall.
appfirewalllogcsrftag perprofilerate	<Double>	Read-only	Rate (/s) counter for appfirewalllogcsrftag perprofile
appfirewalllogxssper profile	<Double>	Read-only	Number of HTML Cross-Site Scripting security check log messages generated by the Application Firewall.
appfirewalllogxssper profilerate	<Double>	Read-only	Rate (/s) counter for appfirewalllogxssper profile
appfirewalllogxformx ssperprofile	<Double>	Read-only	Number of HTML Cross-Site Scripting security check transform log messages generated by the Application Firewall.
appfirewalllogxformx ssperprofilerate	<Double>	Read-only	Rate (/s) counter for appfirewalllogxformx ssperprofile

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
appfirewalllogsqlperprofile	<Double>	Read-only	Number of HTML SQL Injection security check log messages generated by the Application Firewall.
appfirewalllogsqlperprofilerate	<Double>	Read-only	Rate (/s) counter for appfirewalllogsqlperprofile
appfirewalllogxformsqlperprofile	<Double>	Read-only	Number of HTML SQL Injection security check transform log messages generated by the Application Firewall.
appfirewalllogxformsqlperprofilerate	<Double>	Read-only	Rate (/s) counter for appfirewalllogxformsqlperprofile
appfirewalllogfieldformatperprofile	<Double>	Read-only	Number of Field Format security check log messages generated by the Application Firewall.
appfirewalllogfieldformatperprofilerate	<Double>	Read-only	Rate (/s) counter for appfirewalllogfieldformatperprofile
appfirewalllogfieldconsistencyperprofile	<Double>	Read-only	Number of Field Consistency security check log messages generated by the Application Firewall.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
appfirewalllogfieldconsistencyperprofilerate	<Double>	Read-only	Rate (/s) counter for appfirewalllogfieldconsistencyperprofile
appfirewalllogcreditcardperprofile	<Double>	Read-only	Number of Credit Card security check log messages generated by the Application Firewall.
appfirewalllogcreditcardperprofilerate	<Double>	Read-only	Rate (/s) counter for appfirewalllogcreditcardperprofile
appfirewallxformlogcreditcardperprofile	<Double>	Read-only	Number of Credit Card security check transform log messages generated by the Application Firewall.
appfirewallxformlogcreditcardperprofilerate	<Double>	Read-only	Rate (/s) counter for appfirewallxformlogcreditcardperprofile
appfirewalllogsafeobjectperprofile	<Double>	Read-only	Number of Safe Object security check log messages generated by the Application Firewall.
appfirewalllogsafeobjectperprofilerate	<Double>	Read-only	Rate (/s) counter for appfirewalllogsafeobjectperprofile
appfirewalllogcontenttypeperprofile	<Double>	Read-only	Number of Content type security check log messages generated by the Application Firewall.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
appfirewalllogcontent typeperprofilerate	<Double>	Read-only	Rate (/s) counter for appfirewalllogcontent typeperprofile
appfirewalllogsjsond osperprofile	<Double>	Read-only	Number of JSON Denial-of-Service security check log messages generated by the Application Firewall.
appfirewalllogsjsond osperprofilerate	<Double>	Read-only	Rate (/s) counter for appfirewalllogsjsond osperprofile
appfirewalllogsjsons qlperprofile	<Double>	Read-only	Number of JSON SQL Injection security check log messages generated by the Application Firewall.
appfirewalllogsjsons qlperprofilerate	<Double>	Read-only	Rate (/s) counter for appfirewalllogsjsons qlperprofile
appfirewalllogsjsonxs sperprofile	<Double>	Read-only	Number of JSON Cross-Site Scripting (XSS) security check log messages generated by the Application Firewall.
appfirewalllogsjsonxs sperprofilerate	<Double>	Read-only	Rate (/s) counter for appfirewalllogsjsonxs sperprofile
appfirewalllogsjsonc mdperprofile	<Double>	Read-only	Number of JSON Command Injection security check log messages generated

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			by the Application Firewall.
appfirewalllogsjsoncmdperprofilerate	<Double>	Read-only	Rate (/s) counter for appfirewalllogsjsoncmdperprofile
appfirewalllogfileuploadtypesperprofile	<Double>	Read-only	Number of File Upload Types security check log messages generated by the Application Firewall.
appfirewalllogfileuploadtypesperprofilerate	<Double>	Read-only	Rate (/s) counter for appfirewalllogfileuploadtypesperprofile
appfirewallloginfercontenttypexmlpayloadperprofile	<Double>	Read-only	Number of Mismatched Content-Type in request with XML Payload security check logs seen by the Application Firewall.
appfirewallloginfercontenttypexmlpayloadperprofilerate	<Double>	Read-only	Rate (/s) counter for appfirewallloginfercontenttypexmlpayloadperprofile
appfirewalllogcmdperprofile	<Double>	Read-only	Number of HTML Command Injection security check log messages generated by the Application Firewall.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
appfirewalllogcmdperprofilerate	<Double>	Read-only	Rate (/s) counter for appfirewalllogcmdperprofile
appfirewallwellformednesslogsperprofile	<Double>	Read-only	Number of XML Format security check log messages generated by the Application Firewall.
appfirewallwellformednesslogsperprofilerate	<Double>	Read-only	Rate (/s) counter for appfirewallwellformednesslogsperprofile
appfirewallxdoslogsperprofile	<Double>	Read-only	Number of XML Denial-of-Service security check log messages generated by the Application Firewall.
appfirewallxdoslogsperprofilerate	<Double>	Read-only	Rate (/s) counter for appfirewallxdoslogsperprofile
appfirewallmsgvallogsperprofile	<Double>	Read-only	Number of XML Message Validation security check log messages generated by the Application Firewall.
appfirewallmsgvallogsperprofilerate	<Double>	Read-only	Rate (/s) counter for appfirewallmsgvallogsperprofile
appfirewallwsilogsperprofile	<Double>	Read-only	Number of Web Services Interoperability (WS-I) security check log messages generated

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			by the Application Firewall.
appfirewallwsilogsperprofilerate	<Double>	Read-only	Rate (/s) counter for appfirewallwsilogsperprofile
appfirewallxmlsqllogsperprofile	<Double>	Read-only	Number of XML SQL Injection security check log messages generated by the Application Firewall.
appfirewallxmlsqllogsperprofilerate	<Double>	Read-only	Rate (/s) counter for appfirewallxmlsqllogsperprofile
appfirewallxmlxsslogsperprofile	<Double>	Read-only	Number of XML Cross-Site Scripting (XSS) security check log messages generated by the Application Firewall.
appfirewallxmlxsslogsperprofilerate	<Double>	Read-only	Rate (/s) counter for appfirewallxmlxsslogsperprofile
appfirewallxmlattachmentlogsperprofile	<Double>	Read-only	Number of XML Attachment security check log messages generated by the Application Firewall.
appfirewallxmlattachmentlogsperprofilerate	<Double>	Read-only	Rate (/s) counter for appfirewallxmlattachmentlogsperprofile
appfirewallxmlsoapfaultlogsperprofile	<Double>	Read-only	Number of requests generating soap:fault log messages

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
appfirewallxmlsoapfaultlogsperprofilerate	<Double>	Read-only	Rate (/s) counter for appfirewallxmlsoapfaultlogsperprofile
appfirewallxmlgenericlogsperprofile	<Double>	Read-only	Number of requests generating XML Generic log messages
appfirewallxmlgenericlogsperprofilerate	<Double>	Read-only	Rate (/s) counter for appfirewallxmlgenericlogsperprofile
appfirewalllogsqlgramperprofile	<Double>	Read-only	Number of HTML SQL Injection security check log messages (reported by SQL grammar) generated by the Application Firewall.
appfirewalllogsqlgramperprofilerate	<Double>	Read-only	Rate (/s) counter for appfirewalllogsqlgramperprofile
appfirewalllogsjsonsqlgramperprofile	<Double>	Read-only	Number of JSON SQL Injection security check log messages (reported by SQL grammar) generated by the Application Firewall.
appfirewalllogsjsonsqlgramperprofilerate	<Double>	Read-only	Rate (/s) counter for appfirewalllogsjsonsqlgramperprofile
appfirewalllogcmdgramperprofile	<Double>	Read-only	Number of HTML CMD Injection security check log messages (reported

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			by CMD grammar) generated by the Application Firewall.
appfirewalllogcmdgramperprofilerate	<Double>	Read-only	Rate (/s) counter for appfirewalllogcmdgramperprofile
appfirewalllogsjsoncmdgramperprofile	<Double>	Read-only	Number of JSON CMD Injection security check log messages (reported by CMD grammar) generated by the Application Firewall.
appfirewalllogsjsoncmdgramperprofilerate	<Double>	Read-only	Rate (/s) counter for appfirewalllogsjsoncmdgramperprofile
appfirewalllogblockkeywordperprofile	<Double>	Read-only	Number of HTML Block Keyword security check log messages generated by the Application Firewall.
appfirewalllogblockkeywordperprofilerate	<Double>	Read-only	Rate (/s) counter for appfirewalllogblockkeywordperprofile
appfirewalllogjsonblockkeywordperprofile	<Double>	Read-only	Number of JSON Block Keyword security check log messages generated by the Application Firewall.
appfirewalllogjsonblockkeywordperprofilerate	<Double>	Read-only	Rate (/s) counter for appfirewalllogjsonblockkeywordperprofile

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
appfirewalltotallogperprofile	<Double>	Read-only	Number of log messages generated by the application firewall on per profile basis
appfirewalllogperprofilerate	<Double>	Read-only	Rate (/s) counter for appfirewalltotallogperprofile
appfirewallret4xxperprofile	<Double>	Read-only	Number of requests returning HTTP 4xx from the backend server
appfirewallret4xxperprofilerate	<Double>	Read-only	Rate (/s) counter for appfirewallret4xxperprofile
appfirewallret5xxperprofile	<Double>	Read-only	Number of requests returning HTTP 5xx from the backend server
appfirewallret5xxperprofilerate	<Double>	Read-only	Rate (/s) counter for appfirewallret5xxperprofile
appfirewallcfgstarturlclosureperprofile	<Double>	Read-only	Number of profiles with Start URL Closure enabled in the Application Firewall.
appfirewallcfgcookietransformsperprofile	<Double>	Read-only	Number of profiles with Config Cookie Transforms enabled in the Application Firewall.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
appfirewallcfgcrosssitescriptingtransformunsafehtmlperprofile	<Double>	Read-only	Number of profiles with CrossSite Scripting Transform Unsafe HTML enabled in the Application Firewall.
appfirewallcfgcrosssitescriptingcheckcompleteurlsperprofile	<Double>	Read-only	Number of profiles with CrossSite Scripting Check Complete URLs enabled in the Application Firewall.
appfirewallcfgsqlinjectiongrammarperprofile	<Double>	Read-only	Number of profiles with SQL Injection Grammar enabled in the Application Firewall.
appfirewallcfgsqlinjectiontransformspecialcharsperprofile	<Double>	Read-only	Number of profiles with SQL Injection Transform Special Chars enabled in the Application Firewall.
appfirewallcfgsqlinjectionchecksqlwildcharsperprofile	<Double>	Read-only	Number of profiles with SQL Injection Check SQL Wild Chars enabled in the Application Firewall.
appfirewallcfgcreditcardxoutperprofile	<Double>	Read-only	Number of profiles with Credit Card XOut enabled in the Application Firewall.
appfirewallcfgdosecurecreditcardloggingperprofile	<Double>	Read-only	Number of profiles with Do Secure Credit Card Logging

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			enabled in the Application Firewall.
appfirewallcfgstreamingperprofile	<Double>	Read-only	Number of profiles with Streaming enabled in the Application Firewall.
appfirewallcfgtraceperprofile	<Double>	Read-only	Number of profiles with Trace enabled in the Application Firewall.
appfirewallcfgjsonsqlinjectiongrammarperprofile	<Double>	Read-only	Number of profiles with JSON SQL Injection Grammar enabled in the Application Firewall.
appfirewallcfgxmlsqlinjectionchecksqlwildcharsperprofile	<Double>	Read-only	Number of profiles with XML SQL Injection Check SQL Wild Chars enabled in the Application Firewall.
appfirewallcfgusehtmlerrorobjectperprofile	<Double>	Read-only	Number of profiles with Use HTML Error Object enabled in the Application Firewall.
appfirewallcfglogeverypolicyhitperprofile	<Double>	Read-only	Number of profiles with Log Every Policy Hit enabled in the Application Firewall.
appfirewallcfgexemptclosureurlsfromsecuritychecksperprofile	<Double>	Read-only	Number of profiles with Exempt Closure URLs From Security Checks enabled in

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			the Application Firewall.
appfirewallcfgcanonicalizehtmlresponseperprofile	<Double>	Read-only	Number of profiles with Canonicalize HTML Response enabled in the Application Firewall.
appfirewallcfgenableformtaggingperprofile	<Double>	Read-only	Number of profiles with Enable Form Tagging enabled in the Application Firewall.
appfirewallcfgsessionlessurlclosureperprofile	<Double>	Read-only	Number of profiles with Sessionless URL Closure enabled in the Application Firewall.
appfirewallcfgsemicolonfieldseparatorperprofile	<Double>	Read-only	Number of profiles with Semicolon Field Separator enabled in the Application Firewall.
appfirewallcfgexcludefileuploadfromchecksperprofile	<Double>	Read-only	Number of profiles with Exclude File Upload From Checks enabled in the Application Firewall.
appfirewallcfgcheckrequestheadersperprofile	<Double>	Read-only	Number of profiles with Check Request Headers enabled in the Application Firewall.
appfirewallcfgoptimizepartialreqsperprofile	<Double>	Read-only	Number of profiles with Optimize Partial

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Reqs enabled in the Application Firewall.
appfirewallcfgurldecoderequestcookiesperprofile	<Double>	Read-only	Number of profiles with URL Decode Request Cookies enabled in the Application Firewall.
appfirewallcfgpercentdecoderecursivelyperprofile	<Double>	Read-only	Number of profiles with Percent Decode Recursively enabled in the Application Firewall.
appfirewallcfginsertcookiesamesiteattributeperprofile	<Double>	Read-only	Number of profiles with Insert Cookie SameSite Attribute enabled in the Application Firewall.
appfirewallcfgfakeaccountdetectionperprofile	<Double>	Read-only	Number of profiles with Fake Account Detection enabled in the Application Firewall.
appfirewallcfgfieldscanenabledperprofile	<Double>	Read-only	Field Scan enabled in the Application Firewall profile.
appfirewallcfgfieldscanenabledjsonperprofile	<Double>	Read-only	JSON Field Scan enabled in the Application Firewall profile.
appfirewallcfgmessagescanenabledperprofile	<Double>	Read-only	Message Scan enabled in the Application Firewall profile.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
appfirewallcfgmessagescanenabledjsonperprofile	<Double>	Read-only	JSON Message Scan enabled in the Application Firewall profile.

Operations

(click to see Properties)

- GET (ALL)
- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/appfwprofile **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/appfwprofile? **args=name: <String_value> ,detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get appfwprofile resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/appfwprofile? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwprofile": [ {

"name":<String_value>,

"appfirewallviolcombinedxxeperprofile":<Double_value>,

"appfirewallcfgmessagescanenabledjsonperprofile":<Double_value>,

"appfirewalllogcsrftagperprofile":<Double_value>,

"appfirewallwellformednesslogsperprofilerate":<Double_value>,
```

```
"appfirewalllogcreditcardperprofile":<Double_value>,

"appfirewalllogcookiehijackperprofilerate":<Double_value>,

"appfirewalltotalviolperprofile":<Double_value>,

"appfirewallxmlgenericlogsperprofilerate":<Double_value>,

"appfirewallviolxmlsqlviolationsperprofile":<Double_value>,

"appfirewallret5xxperprofile":<Double_value>,

"appfirewallgrpclogsperprofile":<Double_value>,

"appfirewallviolbufferoverflowperprofile":<Double_value>,

"appfirewallgrpclogsperprofilerate":<Double_value>,

"appfirewallabortsperprofilerate":<Double_value>,

"appfirewallvioljsonblockkeywordperprofilerate":<Double_value>,

"appfirewallresponsesperprofile":<Double_value>,

"appfirewallviolcombinedxssperprofile":<Double_value>,

"appfirewallcfgcrosssitescriptingcheckcompleteurlsperprofile":<Double_valu
e>,

"appfirewallloginfercontenttypexmlpayloadperprofile":<Double_value>,

"appfirewallviolcookieperprofile":<Double_value>,

"appfirewalllogrefererheaderperprofile":<Double_value>,

"appfirewallviolxssperprofile":<Double_value>,

"appfirewallpostbodylimitlogsperprofilerate":<Double_value>,

"appfirewallviolcombinedxssperprofilerate":<Double_value>,

"appfirewalllogsjsoncmdperprofilerate":<Double_value>,
```

```
"appfirewallwsilogsperprofile":<Double_value>,

"appfirewallredirectsperprofile":<Double_value>,

"appfirewallcfgusehtmlerrorobjectperprofile":<Double_value>,

"appfirewallxmlsqllogsperprofilerate":<Double_value>,

"appfirewallvioljsoncmdgramperprofilerate":<Double_value>,

"appfirewallviolcmdgramperprofile":<Double_value>,

"appfirewalllogcsrftagperprofilerate":<Double_value>,

"appfirewallviolcreditcardperprofilerate":<Double_value>,

"appfirewallviolfieldconsistencyperprofile":<Double_value>,

"appfirewallviolxmlsoapfaultviolationsperprofilerate":<Double_value>,

"appfirewallpostbodylimitviolationsperprofile":<Double_value>,

"appfirewallreqbytesperprofile":<Double_value>,

"appfirewalllogxformsqlperprofilerate":<Double_value>,

"appfirewallxmlsoapfaultlogsperprofile":<Double_value>,

"appfirewallvioljsonblockkeywordperprofile":<Double_value>,

"appfirewallxmlgenericlogsperprofile":<Double_value>,

"appfirewallviolcombinedowaspperprofile":<Double_value>,

"appfirewallloginfercontenttypexmlpayloadperprofilerate":<Double_value>,

"appfirewallviolwellformednessviolationsperprofilerate":<Double_value>,

"appfirewallviolcookiehijackperprofile":<Double_value>,

"appfirewalllogxformsqlperprofile":<Double_value>,

"appfirewallvioldenyurlperprofilerate":<Double_value>,
```

```
"appfirewallviolcontenttypeperprofile":<Double_value>,

"appfirewallxmlsoapfaultlogsperprofilerate":<Double_value>,

"appfirewallcfgmessagescanenabledperprofile":<Double_value>,

"appfirewallcfgsqlinjectiontransformspecialcharsperprofile":<Double_value>
,

"appfirewallviolxmlxssviolationsperprofile":<Double_value>,

"appfirewallvioljsonsqlgramperprofile":<Double_value>,

"appfirewallviolcreditcardperprofile":<Double_value>,

"appfirewalllogcreditcardperprofilerate":<Double_value>,

"appfirewalllogjsonblockkeywordperprofile":<Double_value>,

"appfirewallxformlogcreditcardperprofilerate":<Double_value>,

"appfirewallviolwellformednessviolationsperprofile":<Double_value>,

"appfirewallviolcmdgramperprofilerate":<Double_value>,

"appfirewallviolfieldconsistencyperprofilerate":<Double_value>,

"appfirewalllogdenyurlperprofile":<Double_value>,

"appfirewalllogrefererheaderperprofilerate":<Double_value>,

"appfirewallcfgfakeaccountdetectionperprofile":<Double_value>,

"appfirewallmsgvallogsperprofile":<Double_value>,

"appfirewallxmlpayloadcontenttypemismatchperprofilerate":<Double_value>,

"appfirewallviolcsrftagperprofilerate":<Double_value>,

"appfirewalllogxformxssperprofilerate":<Double_value>,

"appfirewallviolxssperprofilerate":<Double_value>,
```

```
"appfirewallxmlattachmentlogsperprofile":<Double_value>,

"appfirewalllogsqlgramperprofilerate":<Double_value>,

"appfirewalllogblockkeywordperprofile":<Double_value>,

"appfirewalllogcookieperprofile":<Double_value>,

"appfirewallviolxmlgenericviolationsperprofile":<Double_value>,

"appfirewallcfgcrosssitescriptingtransformunsafehtmlperprofile":<Double_va
lue>,

"appfirewalllogsjsonsqlgramperprofile":<Double_value>,

"appfirewallviolfileuploadtypesperprofile":<Double_value>,

"appfirewallviolxmlsoapfaultviolationsperprofile":<Double_value>,

"appfirewallcfgsqlinjectionchecksqlwildcharsperprofile":<Double_value>,

"appfirewallvioljsonxssperprofilerate":<Double_value>,

"appfirewalllogsafeobjectperprofilerate":<Double_value>,

"appfirewalllogsqlperprofilerate":<Double_value>,

"appfirewalllogfieldformatperprofile":<Double_value>,

"appfirewalllogsjsonxssperprofilerate":<Double_value>,

"appfirewalllogperprofilerate":<Double_value>,

"appfirewallcfgfieldscanenabledjsonperprofile":<Double_value>,

"appfirewallvioljsondosperprofile":<Double_value>,

"appfirewallshortavgresptimeperprofile":<Double_value>,

"appfirewallviolcombinedxxeperprofilerate":<Double_value>,

"appfirewalllogsjsonsqlgramperprofilerate":<Double_value>,
```

```
"appfirewallmsgvallogsperprofilerate":<Double_value>,

"appfirewallvioljsoncmdperprofile":<Double_value>,

"appfirewallviolcmdperprofile":<Double_value>,

"appfirewallviolrefererheaderperprofile":<Double_value>,

"appfirewallcfgcanonicalizehtmlresponseperprofile":<Double_value>,

"appfirewallviolxdosviolationsperprofile":<Double_value>,

"appfirewallviolfieldformatperprofilerate":<Double_value>,

"appfirewallret4xxperprofile":<Double_value>,

"appfirewalllogfileuploadtypesperprofile":<Double_value>,

"appfirewalllogcontenttypeperprofilerate":<Double_value>,

"appfirewalllogsqlperprofile":<Double_value>,

"appfirewallviolsqlgramperprofile":<Double_value>,

"appfirewallviolsafeobjectperprofile":<Double_value>,

"appfirewallxformlogcreditcardperprofile":<Double_value>,

"appfirewallcfgsqlinjectiongrammarperprofile":<Double_value>,

"appfirewalllogdenyurlperprofilerate":<Double_value>,

"appfirewalllogstarturlperprofilerate":<Double_value>,

"appfirewallcfgoptimizepartialreqsperprofile":<Double_value>,

"appfirewallret4xxperprofilerate":<Double_value>,

"appfirewallviolsqlcombinedperprofile":<Double_value>,

"appfirewallviolwsiviolationsperprofile":<Double_value>,

"appfirewalltotallogperprofile":<Double_value>,
```

```
"appfirewallxmlsqllogsperprofile":<Double_value>,

"appfirewallxmlxsslogsperprofilerate":<Double_value>,

"appfirewallcfginsertcookiesamesiteattributeperprofile":<Double_value>,

"appfirewallpostbodylimitlogsperprofile":<Double_value>,

"appfirewalllogbufferoverflowperprofilerate":<Double_value>,

"appfirewallviolfieldformatperprofile":<Double_value>,

"appfirewalllogcookieperprofilerate":<Double_value>,

"appfirewallcfgtraceperprofile":<Double_value>,

"appfirewalllogcookiehijackperprofile":<Double_value>,

"appfirewallviolstarturlperprofilerate":<Double_value>,

"appfirewallabortsperprofile":<Double_value>,

"appfirewallviolmsgvalviolationsperprofilerate":<Double_value>,

"appfirewalllogcmdgramperprofilerate":<Double_value>,

"appfirewalllogsjsonsqlperprofilerate":<Double_value>,

"appfirewallrequestsperprofile":<Double_value>,

"appfirewallcfgsessionlessurlclosureperprofile":<Double_value>,

"appfirewallcfgcookietransformsperprofile":<Double_value>,

"appfirewallviolxmlsqlviolationsperprofilerate":<Double_value>,

"appfirewallxmlxsslogsperprofile":<Double_value>,

"appfirewalllogsjsoncmdperprofile":<Double_value>,

"appfirewalllogblockkeywordperprofilerate":<Double_value>,

"appfirewallviolsignatureperprofile":<Double_value>,
```

```
"appfirewallviolbufferoverflowperprofilerate":<Double_value>,

"appfirewallxmlattachmentlogsperprofilerate":<Double_value>,

"appfirewalllogsjsonsqlperprofile":<Double_value>,

"appfirewallcfglogeverypolicyhitperprofile":<Double_value>,

"appfirewalllogfieldconsistencyperprofilerate":<Double_value>,

"appfirewallcfgenableformtaggingperprofile":<Double_value>,

"appfirewallxdoslogsperprofile":<Double_value>,

"appfirewallviolxmlgenericviolationsperprofilerate":<Double_value>,

"appfirewallcfgjsonsqlinjectiongrammarperprofile":<Double_value>,

"appfirewallret5xxperprofilerate":<Double_value>,

"appfirewallviolxmlattachmentviolationsperprofile":<Double_value>,

"appfirewallcfgdosecurecreditcardloggingperprofile":<Double_value>,

"appfirewalllogfileuploadtypesperprofilerate":<Double_value>,

"appfirewallviolsqlperprofile":<Double_value>,

"appfirewallviolcontenttypeperprofilerate":<Double_value>,

"appfirewallviolmsgvalviolationsperprofile":<Double_value>,

"appfirewallvioljsoncmdgramperprofile":<Double_value>,

"appfirewallcfgxmlsqlinjectionchecksqlwildcharsperprofile":<Double_value>,

"appfirewallviolsafeobjectperprofilerate":<Double_value>,

"appfirewalllongavgresptimeperprofile":<Double_value>,

"appfirewallviolstarturlperprofile":<Double_value>,

"appfirewallpostbodylimitviolationsperprofilerate":<Double_value>,
```

```
"appfirewalllogsjsondosperprofilerate":<Double_value>,

"appfirewallviolcookiehijackperprofilerate":<Double_value>,

"appfirewalllogxformxssperprofile":<Double_value>,

"appfirewallcfgurldecoderequestcookiesperprofile":<Double_value>,

"appfirewallviolcsrftagperprofile":<Double_value>,

"appfirewallvioljsonsqlgramperprofilerate":<Double_value>,

"appfirewallviolblockkeywordperprofile":<Double_value>,

"appfirewallvioljsonsqlperprofile":<Double_value>,

"appfirewallcfgexemptclosureurlsfromsecuritychecksperprofile":<Double_valu
e>,

"appfirewallviolcookieperprofilerate":<Double_value>,

"appfirewallvioljsoncmdperprofilerate":<Double_value>,

"appfirewalllogsjsoncmdgramperprofilerate":<Double_value>,

"appfirewallvioldenyurlperprofile":<Double_value>,

"appfirewallviolrefererheaderperprofilerate":<Double_value>,

"appfirewalllogsjsonxssperprofile":<Double_value>,

"appfirewallviolwsiviolationsperprofilerate":<Double_value>,

"appfirewallviolblockkeywordperprofilerate":<Double_value>,

"appfirewallvioljsonsqlperprofilerate":<Double_value>,

"appfirewallwellformednesslogsperprofile":<Double_value>,

"appfirewallcfgstreamingperprofile":<Double_value>,

"appfirewalllogsqlgramperprofile":<Double_value>,
```

```
"appfirewallresponsesperprofilerate":<Double_value>,

"appfirewallviolxmlattachmentviolationsperprofilerate":<Double_value>,

"appfirewallcfgpercentdecoderecursivelyperprofile":<Double_value>,

"appfirewallviolsignatureperprofilerate":<Double_value>,

"appfirewalllogxssperprofilerate":<Double_value>,

"appfirewallcfgcreditcardxoutperprofile":<Double_value>,

"appfirewallrequestsperprofilerate":<Double_value>,

"appfirewallviolsqlgramperprofilerate":<Double_value>,

"appfirewalllogcmdperprofile":<Double_value>,

"appfirewallredirectsperprofilerate":<Double_value>,

"appfirewalllogcmdperprofilerate":<Double_value>,

"appfirewallcfgsemicolonfieldseparatorperprofile":<Double_value>,

"appfirewalllogsjsondosperprofile":<Double_value>,

"appfirewallreqbytesperprofilerate":<Double_value>,

"appfirewallvioljsonxssperprofile":<Double_value>,

"appfirewalllogxssperprofile":<Double_value>,

"appfirewallcfgstarturlclosureperprofile":<Double_value>,

"appfirewalllogfieldconsistencyperprofile":<Double_value>,

"appfirewallviolperprofilerate":<Double_value>,

"appfirewallviolxmlxssviolationsperprofilerate":<Double_value>,

"appfirewalllogfieldformatperprofilerate":<Double_value>,

"appfirewalllogsafeobjectperprofile":<Double_value>,
```

```
"appfirewalllogcmdgramperprofile":<Double_value>,

"appfirewallresbytesperprofilerate":<Double_value>,

"appfirewallvioljsondosperprofilerate":<Double_value>,

"appfirewalllogcontenttypeperprofile":<Double_value>,

"appfirewallviolsqlcombinedperprofilerate":<Double_value>,

"appfirewallviolxdosviolationsperprofilerate":<Double_value>,

"appfirewallviolfileuploadtypesperprofilerate":<Double_value>,

"appfirewalllogsjsoncmdgramperprofile":<Double_value>,

"appfirewallresbytesperprofile":<Double_value>,

"appfirewallxmlpayloadcontenttypemismatchperprofile":<Double_value>,

"appfirewalllogjsonblockkeywordperprofilerate":<Double_value>,

"appfirewallxdoslogsperprofilerate":<Double_value>,

"appfirewalllogbufferoverflowperprofile":<Double_value>,

"appfirewallcfgfieldscanenabledperprofile":<Double_value>,

"appfirewallviolcombinedowaspperprofilerate":<Double_value>,

"appfirewallviolsqlperprofilerate":<Double_value>,

"appfirewallcfgexcludefileuploadfromchecksperprofile":<Double_value>,

"appfirewallwsilogsperprofilerate":<Double_value>,

"appfirewallcfgcheckrequestheadersperprofile":<Double_value>,

"appfirewalllogstarturlperprofile":<Double_value>,

"appfirewallviolcmdperprofilerate":<Double_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/stat/appfwprofile/ name_value><String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appfwprofile": [ {

"name":<String_value>,

"appfirewallviolcombinedxxeperprofile":<Double_value>,

"appfirewallcfgmessagescanenabledjsonperprofile":<Double_value>,

"appfirewalllogcsrftagperprofile":<Double_value>,

"appfirewallwellformednesslogsperprofilerate":<Double_value>,

"appfirewalllogcreditcardperprofile":<Double_value>,

"appfirewalllogcookiehijackperprofilerate":<Double_value>,

"appfirewalltotalviolperprofile":<Double_value>,

"appfirewallxmlgenericlogsperprofilerate":<Double_value>,

"appfirewallviolxmlsqlviolationsperprofile":<Double_value>,
```

```
"appfirewallret5xxperprofile":<Double_value>,

"appfirewallgrpclogsperprofile":<Double_value>,

"appfirewallviolbufferoverflowperprofile":<Double_value>,

"appfirewallgrpclogsperprofilerate":<Double_value>,

"appfirewallabortsperprofilerate":<Double_value>,

"appfirewallvioljsonblockkeywordperprofilerate":<Double_value>,

"appfirewallresponsesperprofile":<Double_value>,

"appfirewallviolcombinedxssperprofile":<Double_value>,

"appfirewallcfgcrosssitescriptingcheckcompleteurlsperprofile":<Double_valu
e>,

"appfirewallloginfercontenttypexmlpayloadperprofile":<Double_value>,

"appfirewallviolcookieperprofile":<Double_value>,

"appfirewalllogrefererheaderperprofile":<Double_value>,

"appfirewallviolxssperprofile":<Double_value>,

"appfirewallpostbodylimitlogsperprofilerate":<Double_value>,

"appfirewallviolcombinedxssperprofilerate":<Double_value>,

"appfirewalllogsjsoncmdperprofilerate":<Double_value>,

"appfirewallwsilogsperprofile":<Double_value>,

"appfirewallredirectsperprofile":<Double_value>,

"appfirewallcfgusehtmlerrorobjectperprofile":<Double_value>,

"appfirewallxmlsqllogsperprofilerate":<Double_value>,

"appfirewallvioljsoncmdgramperprofilerate":<Double_value>,
```

```
"appfirewallviolcmdgramperprofile":<Double_value>,

"appfirewalllogcsrftagperprofilerate":<Double_value>,

"appfirewallviolcreditcardperprofilerate":<Double_value>,

"appfirewallviolfieldconsistencyperprofile":<Double_value>,

"appfirewallviolxmlsoapfaultviolationsperprofilerate":<Double_value>,

"appfirewallpostbodylimitviolationsperprofile":<Double_value>,

"appfirewallreqbytesperprofile":<Double_value>,

"appfirewalllogxformsqlperprofilerate":<Double_value>,

"appfirewallxmlsoapfaultlogsperprofile":<Double_value>,

"appfirewallvioljsonblockkeywordperprofile":<Double_value>,

"appfirewallxmlgenericlogsperprofile":<Double_value>,

"appfirewallviolcombinedowaspperprofile":<Double_value>,

"appfirewallloginfercontenttypexmlpayloadperprofilerate":<Double_value>,

"appfirewallviolwellformednessviolationsperprofilerate":<Double_value>,

"appfirewallviolcookiehijackperprofile":<Double_value>,

"appfirewalllogxformsqlperprofile":<Double_value>,

"appfirewallvioldenyurlperprofilerate":<Double_value>,

"appfirewallviolcontenttypeperprofile":<Double_value>,

"appfirewallxmlsoapfaultlogsperprofilerate":<Double_value>,

"appfirewallcfgmessagescanenabledperprofile":<Double_value>,

"appfirewallcfgsqlinjectiontransformspecialcharsperprofile":<Double_value>
,
```

```
"appfirewallviolxmlxssviolationsperprofile":<Double_value>,

"appfirewallvioljsonsqlgramperprofile":<Double_value>,

"appfirewallviolcreditcardperprofile":<Double_value>,

"appfirewalllogcreditcardperprofilerate":<Double_value>,

"appfirewalllogjsonblockkeywordperprofile":<Double_value>,

"appfirewallxformlogcreditcardperprofilerate":<Double_value>,

"appfirewallviolwellformednessviolationsperprofile":<Double_value>,

"appfirewallviolcmdgramperprofilerate":<Double_value>,

"appfirewallviolfieldconsistencyperprofilerate":<Double_value>,

"appfirewalllogdenyurlperprofile":<Double_value>,

"appfirewalllogrefererheaderperprofilerate":<Double_value>,

"appfirewallcfgfakeaccountdetectionperprofile":<Double_value>,

"appfirewallmsgvallogsperprofile":<Double_value>,

"appfirewallxmlpayloadcontenttypemismatchperprofilerate":<Double_value>,

"appfirewallviolcsrftagperprofilerate":<Double_value>,

"appfirewalllogxformxssperprofilerate":<Double_value>,

"appfirewallviolxssperprofilerate":<Double_value>,

"appfirewallxmlattachmentlogsperprofile":<Double_value>,

"appfirewalllogsqlgramperprofilerate":<Double_value>,

"appfirewalllogblockkeywordperprofile":<Double_value>,

"appfirewalllogcookieperprofile":<Double_value>,

"appfirewallviolxmlgenericviolationsperprofile":<Double_value>,
```

```
"appfirewallcfgcrosssitescriptingtransformunsafehtmlperprofile":<Double_value>,

"appfirewalllogsjsonsqlgramperprofile":<Double_value>,

"appfirewallviolfileuploadtypesperprofile":<Double_value>,

"appfirewallviolxmlsoapfaultviolationsperprofile":<Double_value>,

"appfirewallcfgsqlinjectionchecksqlwildcharsperprofile":<Double_value>,

"appfirewallvioljsonxssperprofilerate":<Double_value>,

"appfirewalllogsafeobjectperprofilerate":<Double_value>,

"appfirewalllogsqlperprofilerate":<Double_value>,

"appfirewalllogfieldformatperprofile":<Double_value>,

"appfirewalllogsjsonxssperprofilerate":<Double_value>,

"appfirewalllogperprofilerate":<Double_value>,

"appfirewallcfgfieldscanenabledjsonperprofile":<Double_value>,

"appfirewallvioljsondosperprofile":<Double_value>,

"appfirewallshortavgresptimeperprofile":<Double_value>,

"appfirewallviolcombinedxxeperprofilerate":<Double_value>,

"appfirewalllogsjsonsqlgramperprofilerate":<Double_value>,

"appfirewallmsgvallogsperprofilerate":<Double_value>,

"appfirewallvioljsoncmdperprofile":<Double_value>,

"appfirewallviolcmdperprofile":<Double_value>,

"appfirewallviolrefererheaderperprofile":<Double_value>,

"appfirewallcfgcanonicalizehtmlresponseperprofile":<Double_value>,
```

```
"appfirewallviolxdosviolationsperprofile":<Double_value>,

"appfirewallviolfieldformatperprofilerate":<Double_value>,

"appfirewallret4xxperprofile":<Double_value>,

"appfirewalllogfileuploadtypesperprofile":<Double_value>,

"appfirewalllogcontenttypeperprofilerate":<Double_value>,

"appfirewalllogsqlperprofile":<Double_value>,

"appfirewallviolsqlgramperprofile":<Double_value>,

"appfirewallviolsafeobjectperprofile":<Double_value>,

"appfirewallxformlogcreditcardperprofile":<Double_value>,

"appfirewallcfgsqlinjectiongrammarperprofile":<Double_value>,

"appfirewalllogdenyurlperprofilerate":<Double_value>,

"appfirewalllogstarturlperprofilerate":<Double_value>,

"appfirewallcfgoptimizepartialreqsperprofile":<Double_value>,

"appfirewallret4xxperprofilerate":<Double_value>,

"appfirewallviolsqlcombinedperprofile":<Double_value>,

"appfirewallviolwsiviolationsperprofile":<Double_value>,

"appfirewalltotallogperprofile":<Double_value>,

"appfirewallxmlsqllogsperprofile":<Double_value>,

"appfirewallxmlxsslogsperprofilerate":<Double_value>,

"appfirewallcfginsertcookiesamesiteattributeperprofile":<Double_value>,

"appfirewallpostbodylimitlogsperprofile":<Double_value>,

"appfirewalllogbufferoverflowperprofilerate":<Double_value>,
```

```
"appfirewallviolfieldformatperprofile":<Double_value>,

"appfirewalllogcookieperprofilerate":<Double_value>,

"appfirewallcfgtraceperprofile":<Double_value>,

"appfirewalllogcookiehijackperprofile":<Double_value>,

"appfirewallviolstarturlperprofilerate":<Double_value>,

"appfirewallabortsperprofile":<Double_value>,

"appfirewallviolmsgvalviolationsperprofilerate":<Double_value>,

"appfirewalllogcmdgramperprofilerate":<Double_value>,

"appfirewalllogsjsonsqlperprofilerate":<Double_value>,

"appfirewallrequestsperprofile":<Double_value>,

"appfirewallcfgsessionlessurlclosureperprofile":<Double_value>,

"appfirewallcfgcookietransformsperprofile":<Double_value>,

"appfirewallviolxmlsqlviolationsperprofilerate":<Double_value>,

"appfirewallxmlxsslogsperprofile":<Double_value>,

"appfirewalllogsjsoncmdperprofile":<Double_value>,

"appfirewalllogblockkeywordperprofilerate":<Double_value>,

"appfirewallviolsignatureperprofile":<Double_value>,

"appfirewallviolbufferoverflowperprofilerate":<Double_value>,

"appfirewallxmlattachmentlogsperprofilerate":<Double_value>,

"appfirewalllogsjsonsqlperprofile":<Double_value>,

"appfirewallcfglogeverypolicyhitperprofile":<Double_value>,

"appfirewalllogfieldconsistencyperprofilerate":<Double_value>,
```

```
"appfirewallcfgenableformtaggingperprofile":<Double_value>,

"appfirewallxdoslogsperprofile":<Double_value>,

"appfirewallviolxmlgenericviolationsperprofilerate":<Double_value>,

"appfirewallcfgjsonsqlinjectiongrammarperprofile":<Double_value>,

"appfirewallret5xxperprofilerate":<Double_value>,

"appfirewallviolxmlattachmentviolationsperprofile":<Double_value>,

"appfirewallcfgdosecurecreditcardloggingperprofile":<Double_value>,

"appfirewalllogfileuploadtypesperprofilerate":<Double_value>,

"appfirewallviolsqlperprofile":<Double_value>,

"appfirewallviolcontenttypeperprofilerate":<Double_value>,

"appfirewallviolmsgvalviolationsperprofile":<Double_value>,

"appfirewallvioljsoncmdgramperprofile":<Double_value>,

"appfirewallcfgxmlsqlinjectionchecksqlwildcharsperprofile":<Double_value>,

"appfirewallviolsafeobjectperprofilerate":<Double_value>,

"appfirewalllongavgresptimeperprofile":<Double_value>,

"appfirewallviolstarturlperprofile":<Double_value>,

"appfirewallpostbodylimitviolationsperprofilerate":<Double_value>,

"appfirewalllogsjsondosperprofilerate":<Double_value>,

"appfirewallviolcookiehijackperprofilerate":<Double_value>,

"appfirewalllogxformxssperprofile":<Double_value>,

"appfirewallcfgurldecoderequestcookiesperprofile":<Double_value>,

"appfirewallviolcsrftagperprofile":<Double_value>,
```

```
"appfirewallvioljsonsqlgramperprofilerate":<Double_value>,

"appfirewallviolblockkeywordperprofile":<Double_value>,

"appfirewallvioljsonsqlperprofile":<Double_value>,

"appfirewallcfgexemptclosureurlsfromsecuritychecksperprofile":<Double_valu
e>,

"appfirewallviolcookieperprofilerate":<Double_value>,

"appfirewallvioljsoncmdperprofilerate":<Double_value>,

"appfirewalllogsjsoncmdgramperprofilerate":<Double_value>,

"appfirewallvioldenyurlperprofile":<Double_value>,

"appfirewallviolrefererheaderperprofilerate":<Double_value>,

"appfirewalllogsjsonxssperprofile":<Double_value>,

"appfirewallviolwsiviolationsperprofilerate":<Double_value>,

"appfirewallviolblockkeywordperprofilerate":<Double_value>,

"appfirewallvioljsonsqlperprofilerate":<Double_value>,

"appfirewallwellformednesslogsperprofile":<Double_value>,

"appfirewallcfgstreamingperprofile":<Double_value>,

"appfirewalllogsqlgramperprofile":<Double_value>,

"appfirewallresponsesperprofilerate":<Double_value>,

"appfirewallviolxmlattachmentviolationsperprofilerate":<Double_value>,

"appfirewallcfgpercentdecoderecursivelyperprofile":<Double_value>,

"appfirewallviolsignatureperprofilerate":<Double_value>,

"appfirewalllogxssperprofilerate":<Double_value>,
```

```
"appfirewallcfgcreditcardxoutperprofile":<Double_value>,

"appfirewallrequestsperprofilerate":<Double_value>,

"appfirewallviolsqlgramperprofilerate":<Double_value>,

"appfirewalllogcmdperprofile":<Double_value>,

"appfirewallredirectsperprofilerate":<Double_value>,

"appfirewalllogcmdperprofilerate":<Double_value>,

"appfirewallcfgsemicolonfieldseparatorperprofile":<Double_value>,

"appfirewalllogsjsondosperprofile":<Double_value>,

"appfirewallreqbytesperprofilerate":<Double_value>,

"appfirewallvioljsonxssperprofile":<Double_value>,

"appfirewalllogxssperprofile":<Double_value>,

"appfirewallcfgstarturlclosureperprofile":<Double_value>,

"appfirewalllogfieldconsistencyperprofile":<Double_value>,

"appfirewallviolperprofilerate":<Double_value>,

"appfirewallviolxmlxssviolationsperprofilerate":<Double_value>,

"appfirewalllogfieldformatperprofilerate":<Double_value>,

"appfirewalllogsafeobjectperprofile":<Double_value>,

"appfirewalllogcmdgramperprofile":<Double_value>,

"appfirewallresbytesperprofilerate":<Double_value>,

"appfirewallvioljsondosperprofilerate":<Double_value>,

"appfirewalllogcontenttypeperprofile":<Double_value>,

"appfirewallviolsqlcombinedperprofilerate":<Double_value>,
```

```
"appfirewallviolxdosviolationsperprofilerate":<Double_value>,

"appfirewallviolfileuploadtypesperprofilerate":<Double_value>,

"appfirewalllogsjsoncmdgramperprofile":<Double_value>,

"appfirewallresbytesperprofile":<Double_value>,

"appfirewallxmlpayloadcontenttypemismatchperprofile":<Double_value>,

"appfirewalllogjsonblockkeywordperprofilerate":<Double_value>,

"appfirewallxdoslogsperprofilerate":<Double_value>,

"appfirewalllogbufferoverflowperprofile":<Double_value>,

"appfirewallcfgfieldscanenabledperprofile":<Double_value>,

"appfirewallviolcombinedowaspperprofilerate":<Double_value>,

"appfirewallviolsqlperprofilerate":<Double_value>,

"appfirewallcfgexcludefileuploadfromchecksperprofile":<Double_value>,

"appfirewallwsilogsperprofilerate":<Double_value>,

"appfirewallcfgcheckrequestheadersperprofile":<Double_value>,

"appfirewalllogstarturlperprofile":<Double_value>,

"appfirewallviolcmdperprofilerate":<Double_value>

}]}
```

appqoe

Appqoe

Application Level Quality of Experience statistics

NAME	DESCRIPTION
appqoe	Statistics for appqoe.
appqoepolicy	Statistics for AppQoS policy resource.

appqoe

Statistics for appqoe.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full
totinmemrsp	<Double>	Read-only	Total in-memory responses sent from NS
inmemrsprate	<Double>	Read-only	Rate (/s) counter for totinmemrsp
totfaultycookies	<Double>	Read-only	Total faulty cookies received
faultycookiesrate	<Double>	Read-only	Rate (/s) counter for totfaultycookies
totvalidcookies	<Double>	Read-only	Total valid cookies received
validcookiesrate	<Double>	Read-only	Rate (/s) counter for totvalidcookies

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
tothighprireq	<Double>	Read-only	Total Requests served from higher priority queue
highprireqrate	<Double>	Read-only	Rate (/s) counter for tothighprireq
totmediumprireq	<Double>	Read-only	Total Requests served from medium priority queue
mediumprireqrate	<Double>	Read-only	Rate (/s) counter for totmediumprireq
totlowprireq	<Double>	Read-only	Total Requests served from low priority queue
lowprireqrate	<Double>	Read-only	Rate (/s) counter for totlowprireq
totlowestprireq	<Double>	Read-only	Total Requests served from surge priority queue
lowestprireqrate	<Double>	Read-only	Rate (/s) counter for totlowestprireq
totaltsvrsubfailed	<Double>	Read-only	Total number of times alternate server substitution failed
tsvrsubfailedrate	<Double>	Read-only	Rate (/s) counter for totaltsvrsubfailed
totdostrig	<Double>	Read-only	Total number of times HDOS condition triggered

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
dostrigrate	<Double>	Read-only	Rate (/s) counter for totdostrig
totdosqvalidcookies	<Double>	Read-only	Total DOSQ valid cookies received
dosqvalidcookiesrate	<Double>	Read-only	Rate (/s) counter for totdosqvalidcookies
totdoshvalidcookies	<Double>	Read-only	Total DOSH valid cookies received
doshvalidcookiesrate	<Double>	Read-only	Rate (/s) counter for totdoshvalidcookies
totsidvalidcookies	<Double>	Read-only	Total SID valid cookies received
sidvalidcookiesrate	<Double>	Read-only	Rate (/s) counter for totsidvalidcookies
totonhvalidcookies	<Double>	Read-only	Total ONH valid cookies received
onhvalidcookiesrate	<Double>	Read-only	Rate (/s) counter for totonhvalidcookies
totpriqvalidcookies	<Double>	Read-only	Total PRIQ valid cookies received
priqvalidcookiesrate	<Double>	Read-only	Rate (/s) counter for totpriqvalidcookies
totdosqfaultycookies	<Double>	Read-only	Total DOSQ faulty cookies received
dosqfaultycookiesrate	<Double>	Read-only	Rate (/s) counter for totdosqfaultycookies
totdoshfaultycookies	<Double>	Read-only	Total DOSH faulty cookies received

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
doshfaultycookiesrate	<Double>	Read-only	Rate (/s) counter for totdoshfaultycookies
totsidfaultycookies	<Double>	Read-only	Total SID faulty cookies received
sidfaultycookiesrate	<Double>	Read-only	Rate (/s) counter for totsidfaultycookies
totonhfaultycookies	<Double>	Read-only	Total ONH faulty cookies received
onhfaultycookiesrate	<Double>	Read-only	Rate (/s) counter for totonhfaultycookies
totpriqfaultycookies	<Double>	Read-only	Total PRIQ faulty cookies received
priqfaultycookiesrate	<Double>	Read-only	Rate (/s) counter for totpriqfaultycookies
totpriembedlinks	<Double>	Read-only	Total requests for valid embedded links
priembedlinksrate	<Double>	Read-only	Rate (/s) counter for totpriembedlinks
totsessreq	<Double>	Read-only	Total valid SIDQ requests within session
sessreqrate	<Double>	Read-only	Rate (/s) counter for totsessreq
totaltcntreq	<Double>	Read-only	Total requests for alternate contents
tcntreqrate	<Double>	Read-only	Rate (/s) counter for totaltcntreq

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
totgetinmemrsp	<Double>	Read-only	Total in-memory GET responses sent from NS
getinmemrsprate	<Double>	Read-only	Rate (/s) counter for totgetinmemrsp
totpostinmemrsp	<Double>	Read-only	Total in-memory POST responses sent from NS
postinmemrsprate	<Double>	Read-only	Rate (/s) counter for totpostinmemrsp
totpostinmemrspbytes	<Double>	Read-only	Total in-memory response bytes sent from NS
postinmemrspbytesrate	<Double>	Read-only	Rate (/s) counter for totpostinmemrspbytes

Operations

(click to see Properties)

- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of

creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/appqoe **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/appqoe? **args=detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get appqoe resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/appqoe? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appqoe": [ {

"postinmemrspbytesrate":<Double_value>,

"priqvalidcookiesrate":<Double_value>,

"totaltcntreq":<Double_value>,

"totonhvalidcookies":<Double_value>,

"lowprireqrate":<Double_value>,

"totlowestprireq":<Double_value>,

"tsvrsubfailedrate":<Double_value>,

"totsidvalidcookies":<Double_value>,

"mediumprireqrate":<Double_value>,

"dosqfaultycookiesrate":<Double_value>,

"dostrigrate":<Double_value>,

"totpriembedlinks":<Double_value>,

"tothighprireq":<Double_value>,

"validcookiesrate":<Double_value>,

"totdostrig":<Double_value>,

"totinmemrsp":<Double_value>,

"totdosqvalidcookies":<Double_value>,

"totgetinmemrsp":<Double_value>,

"dosqvalidcookiesrate":<Double_value>,

"totdosqfaultycookies":<Double_value>,

"totsidfaultycookies":<Double_value>,
```

```
"priqfaultycookiesrate":<Double_value>,

"totlowprireq":<Double_value>,

"postinmemrsprate":<Double_value>,

"totfaultycookies":<Double_value>,

"totonhfaultycookies":<Double_value>,

"doshvalidcookiesrate":<Double_value>,

"onhvalidcookiesrate":<Double_value>,

"sessreqrate":<Double_value>,

"sidfaultycookiesrate":<Double_value>,

"totdoshfaultycookies":<Double_value>,

"totvalidcookies":<Double_value>,

"totdoshvalidcookies":<Double_value>,

"getinmemrsprate":<Double_value>,

"totsessreq":<Double_value>,

"inmemrsprate":<Double_value>,

"sidvalidcookiesrate":<Double_value>,

"lowestprireqrate":<Double_value>,

"highprireqrate":<Double_value>,

"totpriqvalidcookies":<Double_value>,

"totpriqfaultycookies":<Double_value>,

"totpostinmemrspbytes":<Double_value>,

"tcntreqrate":<Double_value>,
```

```
"onhfaultycookiesrate":<Double_value>,

"totpostinmemrsp":<Double_value>,

"totmediumprireq":<Double_value>,

"doshfaultycookiesrate":<Double_value>,

"priembedlinksrate":<Double_value>,

"faultycookiesrate":<Double_value>,

"totaltsvrsubfailed":<Double_value>

}]}
```

appqoepolicy

Statistics for AppQoS policy resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	policyName. Minimum length = 1
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full
qosavgserverttfb	<Double>	Read-only	Average Server Time-To-First-Byte in milliseconds calculated for this AppQoE policy.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
qosavgserverttfbrate	<Double>	Read-only	Rate (/s) counter for qosavgserverttfb
qosavgserverttlb	<Double>	Read-only	Average Server Time-To-Last-Byte in milliseconds calculated for this AppQoE policy.
qosavgserverttlbrate	<Double>	Read-only	Rate (/s) counter for qosavgserverttlb
qosavgclientttlb	<Double>	Read-only	Average Client Time-To-Last-Byte in milliseconds calculated for this AppQoE policy.
qosavgclientttlbrate	<Double>	Read-only	Rate (/s) counter for qosavgclientttlb
totthroughput	<Double>	Read-only	Throughput in Kbps calculated on this AppQoE policy
throughputrate	<Double>	Read-only	Rate (/s) counter for totthroughput
totsvrlinkedto	<Double>	Read-only	Total number of server connections that were established through this AppQoE Policy
svrlinkedtorate	<Double>	Read-only	Rate (/s) counter for totsvrlinkedto
totcltrequests	<Double>	Read-only	Total number of client connections that were requested

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			through this AppQoE Policy
cltrequestsrate	<Double>	Read-only	Rate (/s) counter for totcltrequests
totrequests	<Double>	Read-only	Total number of requests that were requested through this AppQoE policy
requestsrate	<Double>	Read-only	Rate (/s) counter for totrequests
totrequestbytes	<Double>	Read-only	Total number of requests bytes that were requested through this AppQoE policy
requestbytesrate	<Double>	Read-only	Rate (/s) counter for totrequestbytes
totresponse	<Double>	Read-only	Total number of responses received by this AppQoE policy
responserate	<Double>	Read-only	Rate (/s) counter for totresponse
totresponsebytes	<Double>	Read-only	Total number of response bytes received by this AppQoE policy
responsebytesrate	<Double>	Read-only	Rate (/s) counter for totresponsebytes
totjssent	<Double>	Read-only	Total number of in-memory responses sent instead of

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			expected responses through this AppQoE policy
jssentrate	<Double>	Read-only	Rate (/s) counter for totjssent
totjsbytessent	<Double>	Read-only	Total bytes of in-memory responses sent through this AppQoE policy
jsbytessentrate	<Double>	Read-only	Rate (/s) counter for totjsbytessent
pipolicyhits	<Double>	Read-only	Number of hits on the policy
pipolicyhitsrate	<Double>	Read-only	Rate (/s) counter for pipolicyhits

Operations

(click to see Properties)

- GET (ALL)
- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.
- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of

creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/appqoepolicy **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/appqoepolicy? **args=name: <String_value> ,detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get appqoepolicy resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/appqoepolicy? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appqoepolicy": [ {

"name":<String_value>,

"requestsrate":<Double_value>,

"qosavgserverttlbrate":<Double_value>,

"qosavgserverttlb":<Double_value>,

"throughputrate":<Double_value>,

"totcltrequests":<Double_value>,

"totresponsebytes":<Double_value>,

"pipolicyhits":<Double_value>,

"totjssent":<Double_value>,

"pipolicyhitsrate":<Double_value>,

"totsvrlinkedto":<Double_value>,

"jsbytessentrate":<Double_value>,

"totjsbytessent":<Double_value>,

"cltrequestsrate":<Double_value>,

"svrlinkedtorate":<Double_value>,

"responserate":<Double_value>,

"requestbytesrate":<Double_value>,

"qosavgserverttfbrate":<Double_value>,

"totresponse":<Double_value>,

"totthroughput":<Double_value>,
```

```
"qosavgserverttfb":<Double_value>,

"jssentrate":<Double_value>,

"totrequestbytes":<Double_value>,

"qosavgclientttlb":<Double_value>,

"totrequests":<Double_value>,

"qosavgclientttlbrate":<Double_value>,

"responsebytesrate":<Double_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/stat/appqoepolicy/ name_value><String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "appqoepolicy": [ {

"name":<String_value>,

"requestsrate":<Double_value>,
```

```
"qosavgserverttlbrate":<Double_value>,

"qosavgserverttlb":<Double_value>,

"throughputrate":<Double_value>,

"totcltrequests":<Double_value>,

"totresponsebytes":<Double_value>,

"pipolicyhits":<Double_value>,

"totjssent":<Double_value>,

"pipolicyhitsrate":<Double_value>,

"totsvrlinkedto":<Double_value>,

"jsbytessentrate":<Double_value>,

"totjsbytessent":<Double_value>,

"cltrequestsrate":<Double_value>,

"svrlinkedtorate":<Double_value>,

"responserate":<Double_value>,

"requestbytesrate":<Double_value>,

"qosavgserverttfbrate":<Double_value>,

"totresponse":<Double_value>,

"totthroughput":<Double_value>,

"qosavgserverttfb":<Double_value>,

"jssentrate":<Double_value>,

"totrequestbytes":<Double_value>,

"qosavgclientttlb":<Double_value>,
```

```
"totrequests":<Double_value>,

"qosavgclientttlbrate":<Double_value>,

"responsebytesrate":<Double_value>

}]}
```

audit

Audit

Audit statistics.

NAME	DESCRIPTION
audit	Statistics for audit.

audit

Statistics for audit.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full
auditsyslogmsgsent	<Double>	Read-only	Syslog messages sent to the syslog server(s) over UDP.
auditsyslogmsgsentrate	<Double>	Read-only	Rate (/s) counter for auditsyslogmsgsent

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
auditsyslogmsggen	<Double>	Read-only	Syslog messages about to be sent to the syslog server.
auditsyslogmsggenrate	<Double>	Read-only	Rate (/s) counter for auditsyslogmsggen
auditsyslogmsgsenttcp	<Double>	Read-only	Syslog messages sent to the syslog server(s) over TCP.
auditsyslogmsgsenttcprate	<Double>	Read-only	Rate (/s) counter for auditsyslogmsgsenttcp
auditjsonobjcreated	<Double>	Read-only	Total number of JSON objects created for HTTP based syslog servers
auditjsonobjcreatedrate	<Double>	Read-only	Rate (/s) counter for auditjsonobjcreated
auditjsonbufexported	<Double>	Read-only	Total number of JSON buffers exported for HTTP based syslog servers
auditjsonbufexportedrate	<Double>	Read-only	Rate (/s) counter for auditjsonbufexported
auditjson2xxresp	<Double>	Read-only	Total number of 2xx responses received for HTTP based syslog servers
auditjson2xxresprate	<Double>	Read-only	Rate (/s) counter for auditjson2xxresp
auditjsonnon2xxresp	<Double>	Read-only	Total number of non 2xx responses

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			received for HTTP based syslog servers
auditjsonnon2xxresp rate	<Double>	Read-only	Rate (/s) counter for auditjsonnon2xxresp
auditsyslogmsgsente xternal	<Double>	Read-only	Syslog messages sent to external syslog server(s) over UDP.
auditsyslogmsgsente xternalrate	<Double>	Read-only	Rate (/s) counter for auditsyslogmsgsente xternal
auditnsballocfail	<Double>	Read-only	NAT allocation failed.
auditnsballocfailrate	<Double>	Read-only	Rate (/s) counter for auditnsballocfail
auditlog32errsyslogal locnsbfail	<Double>	Read-only	Nsb allocation failed.
auditlog32errsyslogal locnsbfailrate	<Double>	Read-only	Rate (/s) counter for auditlog32errsyslogal locnsbfail
auditmemallocfail	<Double>	Read-only	Failures in allocation of Access Gateway context structure. When an Access Gateway session is established, the Citrix ADC creates an internal context structure , which identifies the user and the IP address from which the user has logged in.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
auditmemallocfailrate	<Double>	Read-only	Rate (/s) counter for auditmemallocfail
auditportallocfail	<Double>	Read-only	Number of times the Citrix ADC failed to allocate a port when sending a syslog message to the syslog server(s).
auditportallocfailrate	<Double>	Read-only	Rate (/s) counter for auditportallocfail
auditcontextnotfound	<Double>	Read-only	Failures in finding the context structure for an Access Gateway session during attempts to send session-specific audit messages.

During an Access Gateway session, audit messages related to the session are queued up in the auditlog buffer for transmission to the audit log server(s). If the session is killed before the messages are sent, the context structure allocated at session creation is removed. This structure is needed for sending the queued auditlog messages. If it is not found, this counter is incremented.

Operations

(click to see Properties)

- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/audit **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/audit? **args=detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get audit resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/audit? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "audit": [ {

"nsbchainallocfailrate":<Double_value>,

"logunsentlbsys":<Double_value>,

"auditjsonobjcreateerrrate":<Double_value>,

"auditjsonnon2xxresprate":<Double_value>,

"auditportallocfail":<Double_value>,

"auditnsballocfailrate":<Double_value>,

"systcpconnfail":<Double_value>,

"auditjsonbufexporterrrate":<Double_value>,

"auditsyslogmsggen":<Double_value>,

"auditlog32errsyslogallocnsbfail":<Double_value>,

"logsdroppedtxminnsbsrate":<Double_value>,

"auditjsonobjcreated":<Double_value>,

"auditsyslogmsgsenttcp":<Double_value>,

"flushcmdcnt":<Double_value>,

"systcpconnfailrate":<Double_value>,

"nsbchainallocfail":<Double_value>,

"logunsentlbsysrate":<Double_value>,

"auditsyslogmsggenrate":<Double_value>,
```

```
"auditsyslogmsgsent":<Double_value>,

"logsdroppedrate":<Double_value>,

"auditjsonobjcreateerr":<Double_value>,

"auditnsballocfail":<Double_value>,

"auditlog32errsyslogallocnsbfailrate":<Double_value>,

"logsdroppedtxminnsbs":<Double_value>,

"logsdropped":<Double_value>,

"auditjson2xxresprate":<Double_value>,

"auditcontextnotfoundrate":<Double_value>,

"auditjsonobjcreatedrate":<Double_value>,

"clientconnfailrate":<Double_value>,

"auditjson2xxresp":<Double_value>,

"auditmemallocfail":<Double_value>,

"auditportallocfailrate":<Double_value>,

"auditcontextnotfound":<Double_value>,

"auditjsonbufexporterr":<Double_value>,

"auditsyslogmsgsentexternal":<Double_value>,

"flushcmdcntrate":<Double_value>,

"auditsyslogmsgsentexternalrate":<Double_value>,

"auditjsonbufexportedrate":<Double_value>,

"auditmemallocfailrate":<Double_value>,

"auditsyslogmsgsentrate":<Double_value>,
```

```
"auditsyslogmsgsenttcprate":<Double_value>,

"auditjsonbufexported":<Double_value>,

"clientconnfail":<Double_value>,

"auditjsonnon2xxresp":<Double_value>

}]}
```

authentication

Authentication

Authentication statistics.

NAME	DESCRIPTION
authenticationloginschemapolicy	
authenticationoauthidppolicy	Statistics for AAA OAuth IdentityProvider (IdP) policy resource.
authenticationpolicy	Statistics for Authentication Policy resource.
authenticationpolicylabel	Statistics for authentication policy label resource.
authenticationsamlidppolicy	Statistics for AAA Saml IdentityProvider (IdP) policy resource.
authenticationvserver	Statistics for authentication virtual server resource.

authenticationloginschemapolicy

Read/write properties

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	The name of the LoginSchema policy for which statistics will be displayed. If not given statistics are shown for all policies. Minimum length = 1
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full
pipolicyhits	<Double>	Read-only	Number of hits on the policy
pipolicyhitsrate	<Double>	Read-only	Rate (/s) counter for pipolicyhits
pipolicyundefhits	<Double>	Read-only	Number of undef hits on the policy
pipolicyundefhitsrate	<Double>	Read-only	Rate (/s) counter for pipolicyundefhits

Operations

(click to see Properties)

- GET (ALL)
- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/authenticationloginschemapolicy **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/authenticationloginschemapolicy? **args=name: <String_value> ,detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get authenticationloginschemapolicy resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/authenticationloginschemapolicy? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationloginschemapolicy": [ {

"name":<String_value>,

"pipolicyundefhitsrate":<Double_value>,

"pipolicyhitsrate":<Double_value>,

"pipolicyundefhits":<Double_value>,

"pipolicyhits":<Double_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/stat/authenticationloginschemapolicy/ name_value><String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationloginschemapolicy": [ {

"name":<String_value>,

"pipolicyundefhitsrate":<Double_value>,

"pipolicyhitsrate":<Double_value>,

"pipolicyundefhits":<Double_value>,

"pipolicyhits":<Double_value>

}]}
```

authenticationoauthidppolicy

Statistics for AAA OAuth IdentityProvider (IdP) policy resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	The name of the OAuth Identity Provider (IdP) policy for which statistics will be displayed. If not given statistics are shown for all policies. Minimum length = 1
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full
pipolicyhits	<Double>	Read-only	Number of hits on the policy

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
pipolicyhitsrate	<Double>	Read-only	Rate (/s) counter for pipolicyhits
pipolicyundefhits	<Double>	Read-only	Number of undef hits on the policy
pipolicyundefhitsrate	<Double>	Read-only	Rate (/s) counter for pipolicyundefhits

Operations

(click to see Properties)

- GET (ALL)
- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.
- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/authenticationoauthidppolicy **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/authenticationoauthidppolicy? **args=name: <String_value> ,detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get authenticationoauthidppolicy resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/authenticationoauthidppolicy? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationoauthidppolicy": [ {

"name":<String_value>,

"pipolicyundefhits":<Double_value>,

"pipolicyhits":<Double_value>,

"pipolicyundefhitsrate":<Double_value>,
```

```
"pipolicyhitsrate":<Double_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/stat/authenticationoauthidppolicy/ name_value><String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationoauthidppolicy": [ {

"name":<String_value>,

"pipolicyundefhits":<Double_value>,

"pipolicyhits":<Double_value>,

"pipolicyundefhitsrate":<Double_value>,

"pipolicyhitsrate":<Double_value>

}]}
```

authenticationpolicy

Statistics for Authentication Policy resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the advanced authentication policy for which to display statistics. If no name is specified, statistics for all advanced authentication polices are shown. Minimum length = 1
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full
pipolicyhits	<Double>	Read-only	Number of hits on the policy
pipolicyhitsrate	<Double>	Read-only	Rate (/s) counter for pipolicyhits
pipolicyundefhits	<Double>	Read-only	Number of undef hits on the policy
pipolicyundefhitsrate	<Double>	Read-only	Rate (/s) counter for pipolicyundefhits

Operations

(click to see Properties)

- GET (ALL)
- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/authenticationpolicy **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/authenticationpolicy? **args=name: <String_value> ,detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get authenticationpolicy resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/authenticationpolicy? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationpolicy": [ {

"name":<String_value>,

"pipolicyundefhits":<Double_value>,

"pipolicyhits":<Double_value>,

"pipolicyundefhitsrate":<Double_value>,

"pipolicyhitsrate":<Double_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/stat/authenticationpolicy/ name_value><String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationpolicy": [ {

"name":<String_value>,

"pipolicyundefhits":<Double_value>,

"pipolicyhits":<Double_value>,

"pipolicyundefhitsrate":<Double_value>,

"pipolicyhitsrate":<Double_value>

}]}
```

authenticationpolicylabel

Statistics for authentication policy label resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
labelname	<String>	Read-write	Name of the authentication policy label. Minimum length = 1
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
pipolicylabelhits	<Double>	Read-only	Number of times policy label was invoked.
pipolicylabelhitsrate	<Double>	Read-only	Rate (/s) counter for pipolicylabelhits

Operations

(click to see Properties)

- GET (ALL)
- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/authenticationpolicylabel **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/authenticationpolicylabel? **args=labelname: <String_value> ,detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get authenticationpolicylabel resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/authenticationpolicylabel? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationpolicylabel": [ {

"labelname":<String_value>,

"pipolicylabelhits":<Double_value>,

"pipolicylabelhitsrate":<Double_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/stat/authenticationpolicylabel/ labelname_value><String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationpolicylabel": [ {

"labelname":<String_value>,

"pipolicylabelhits":<Double_value>,

"pipolicylabelhitsrate":<Double_value>

}]}
```

authenticationsamlidppolicy

Statistics for AAA Saml IdentityProvider (IdP) policy resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	The name of the SAML Identity

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Provider (IdP) policy for which statistics will be displayed. If not given statistics are shown for all policies. Minimum length = 1
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full
pipolicyhits	<Double>	Read-only	Number of hits on the policy
pipolicyhitsrate	<Double>	Read-only	Rate (/s) counter for pipolicyhits

Operations

(click to see Properties)

- GET (ALL)
- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/authenticationsamlidppolicy **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/authenticationsamlidppolicy? **args=name: <String_value> ,detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get authenticationsamlidppolicy resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/authenticationsamlidppolicy? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationsamlidppolicy": [ {

"name":<String_value>,

"pipolicyhitsrate":<Double_value>,

"pipolicyhits":<Double_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/stat/authenticationsamlidppolicy/ name_value><String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationsamlidppolicy": [ {

"name":<String_value>,

"pipolicyhitsrate":<Double_value>,

"pipolicyhits":<Double_value>

}]}
```

authenticationvserver

Statistics for authentication virtual server resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the authentication virtual server. Minimum length = 1
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full
primaryipaddress	<String>	Read-only	The IP address on which the service is running.
primaryport	<Integer>	Read-only	The port on which the service is running.
type	<String>	Read-only	Protocol associated with the vserver
state	<String>	Read-only	Current state of the server. There are seven possible values: UP(7), DOWN(1), UNKNOWN(2), BUSY(3), OFS(Out of Service)(4), TROFS(Transition Out of Service)(5), TROFS_DOWN(Down When going Out of Service)(8)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
totalrequests	<Double>	Read-only	Total number of requests received on this service or virtual server. (This applies to HTTP/SSL services and servers.)
requestsrate	<Double>	Read-only	Rate (/s) counter for totalrequests
totalresponses	<Double>	Read-only	Number of responses received on this service or virtual server. (This applies to HTTP/SSL services and servers.)
responsesrate	<Double>	Read-only	Rate (/s) counter for totalresponses
totalrequestbytes	<Double>	Read-only	Total number of request bytes received on this service or virtual server.
requestbytesrate	<Double>	Read-only	Rate (/s) counter for totalrequestbytes
totalresponsebytes	<Double>	Read-only	Number of response bytes received by this service or virtual server.
responsebytesrate	<Double>	Read-only	Rate (/s) counter for totalresponsebytes

Operations

(click to see Properties)

- GET (ALL)
- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/authenticationvserver **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/authenticationvserver? **args=name: <String_value> ,detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get authenticationvserver resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/authenticationvserver? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationvserver": [ {

"name":<String_value>,

"totalrequestbytes":<Double_value>,

"requestsrate":<Double_value>,

"primaryport":<Integer_value>,

"totalrequests":<Double_value>,

"responsesrate":<Double_value>,

"requestbytesrate":<Double_value>,

"totalresponses":<Double_value>,

"totalresponsebytes":<Double_value>,

"primaryipaddress":<String_value>,

"type":<String_value>,

"responsebytesrate":<Double_value>,
```

```
"state":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/stat/authenticationvserver/ name_value><String>
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authenticationvserver": [ {

"name":<String_value>,

"totalrequestbytes":<Double_value>,

"requestsrate":<Double_value>,

"primaryport":<Integer_value>,

"totalrequests":<Double_value>,

"responsesrate":<Double_value>,

"requestbytesrate":<Double_value>,

"totalresponses":<Double_value>,
```

```
"totalresponsebytes":<Double_value>,

"primaryipaddress":<String_value>,

"type":<String_value>,

"responsebytesrate":<Double_value>,

"state":<String_value>

}]}
```

authorization

Authorization

Authorization statistics. Authorization services check which resources users are authorized to access, and grant permissions accordingly.

NAME	DESCRIPTION
authorizationpolicylabel	Statistics for authorization policy label resource.

authorizationpolicylabel

Statistics for authorization policy label resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
labelname	<String>	Read-write	Name of the authorization policy label. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full
pipolicylabelhits	<Double>	Read-only	Number of times policy label was invoked.
pipolicylabelhitsrate	<Double>	Read-only	Rate (/s) counter for pipolicylabelhits

Operations

(click to see Properties)

- GET (ALL)
- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/authorizationpolicylabel **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/authorizationpolicylabel? **args=labelname: <String_value> ,detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get authorizationpolicylabel resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/authorizationpolicylabel? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authorizationpolicylabel": [ {

"labelname":<String_value>,

"pipolicylabelhitsrate":<Double_value>,

"pipolicylabelhits":<Double_value>
```

```
}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/stat/authorizationpolicylabel/ labelname_value><String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "authorizationpolicylabel": [ {

"labelname":<String_value>,

"pipolicylabelhitsrate":<Double_value>,

"pipolicylabelhits":<Double_value>

}]}
```

autoscale

Autoscale

AutoScale statistics.

NAME	DESCRIPTION
autoscalepolicy	Statistics for Autoscale policy resource.

autoscalepolicy

Statistics for Autoscale policy resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	The name of the autoscale policy for which statistics will be displayed. If not given statistics are shown for all autoscale policies. Minimum length = 1
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full
pipolicyhits	<Double>	Read-only	Number of hits on the policy
pipolicyhitsrate	<Double>	Read-only	Rate (/s) counter for pipolicyhits
pipolicyundefhits	<Double>	Read-only	Number of undef hits on the policy
pipolicyundefhitsrate	<Double>	Read-only	Rate (/s) counter for pipolicyundefhits

Operations

(click to see Properties)

- GET (ALL)
- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/autoscalepolicy **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/autoscalepolicy? **args=name: <String_value> ,detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get autoscalepolicy resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/autoscalepolicy? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "autoscalepolicy": [ {

"name":<String_value>,

"pipolicyhitsrate":<Double_value>,

"pipolicyundefhitsrate":<Double_value>,

"pipolicyhits":<Double_value>,

"pipolicyundefhits":<Double_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/stat/autoscalepolicy/ name_value><String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "autoscalepolicy": [ {

"name":<String_value>,

"pipolicyhitsrate":<Double_value>,

"pipolicyundefhitsrate":<Double_value>,

"pipolicyhits":<Double_value>,

"pipolicyundefhits":<Double_value>

}]}
```

basic

Basic

Basic system statistics.

NAME	DESCRIPTION
service	Statistics for service resource.
servicegroup	Statistics for service group resource.
servicegroupmember	Statistics for service group entity resource.

service

Statistics for service resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the service. Minimum length = 1
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full
throughput	<Double>	Read-only	Number of bytes received or sent by this service (Mbps).
throughputrate	<Double>	Read-only	Rate (/s) counter for throughput
avgsvrttfb	<Double>	Read-only	Average TTFB between the Citrix ADC and the server. TTFB is the time interval between sending the request packet to a service and receiving the first response from the service
primaryipaddress	<String>	Read-only	The IP address on which the service is running.
primaryport	<Integer>	Read-only	The port on which the service is running.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
servicetype	<String>	Read-only	The service type of this service.Possible values are ADNS, DNS, MYSQL, RTSP, SSL_DIAMETER, ADNS_TCP, DNS_TCP, NNTP, SIP_UDP, SSL_TCP, ANY, FTP, RADIUS, SNMP, TCP, DHCPRA, HTTP, RDP, SSL, TFTP, DIAMETER, MSSQL, RPCSVR, SSL_BRIDGE, UDP
state	<String>	Read-only	Current state of the server. There are seven possible values: UP(7), DOWN(1), UNKNOWN(2), BUSY(3), OFS(Out of Service)(4), TROFS(Transition Out of Service)(5), TROFS_DOWN(Down When going Out of Service)(8)
totalrequests	<Double>	Read-only	Total number of requests received on this service or virtual server. (This applies to HTTP/SSL services and servers.)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
requestsrate	<Double>	Read-only	Rate (/s) counter for totalrequests
totalresponses	<Double>	Read-only	Number of responses received on this service or virtual server. (This applies to HTTP/SSL services and servers.)
responsesrate	<Double>	Read-only	Rate (/s) counter for totalresponses
totalrequestbytes	<Double>	Read-only	Total number of request bytes received on this service or virtual server.
requestbytesrate	<Double>	Read-only	Rate (/s) counter for totalrequestbytes
totalresponsebytes	<Double>	Read-only	Number of response bytes received by this service or virtual server.
responsebytesrate	<Double>	Read-only	Rate (/s) counter for totalresponsebytes
curclntconnections	<Double>	Read-only	Number of current client connections.
surgecount	<Double>	Read-only	Number of requests in the surge queue.
cursrvrconnections	<Double>	Read-only	Number of current connections to the actual servers

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			behind the virtual server.
svrestablishedconn	<Double>	Read-only	Number of server connections in ESTABLISHED state.
curreusepool	<Double>	Read-only	Number of requests in the idle queue/ reuse pool.
maxclients	<Double>	Read-only	Maximum open connections allowed on this service.
curload	<Double>	Read-only	Load on the service that is calculated from the bound load based monitor.
totalconnreassembly queue75	<Double>	Read-only	Total no of connections with 75% TCP reassembly queue
totalconnreassembly queueflush	<Double>	Read-only	Total no of connections incurred TCP reassembly queue flush
httpmaxhdrszpkts	<Double>	Read-only	Number of http max header size packet parsing failures
httpmaxhdrfldlenpkts	<Double>	Read-only	Number of HTTP requests exceeding max header field length

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
tcpmaxooopkts	<Double>	Read-only	No of times max out of order packets reached
curtflags	<Double>	Read-only	Current flags on the service for internal use in display handlers.
totsvrttlbtransactions	<Double>	Read-only	Total transactions where server TTLB is calculated.
toleratingttlbtransactions	<Double>	Read-only	Tolerable transactions based on APDEX threshold (>T ;; <4T).
frustratingttlbtransactions	<Double>	Read-only	Frustrating transactions based on APDEX threshold (>4T).
vsvrservicehits	<Double>	Read-only	Number of times that the service has been provided.
vsvrservicehitsrate	<Double>	Read-only	Rate (/s) counter for vsvrservicehits
activetransactions	<Double>	Read-only	Number of active transactions handled by this service. (Including those in the surge queue.) Active Transaction means number of transactions currently served by the server including

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			those waiting in the SurgeQ
serviceorder	<Double>	Read-only	Order with which service is bound to vserver

Operations

(click to see Properties)

- GET (ALL)
- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/service **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/service? **args=name: <String_value> ,detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get service resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/service? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "service": [ {

"name":<String_value>,

"cursrvrconnections":<Double_value>,

"tcpmaxooopkts":<Double_value>,

"curtflags":<Double_value>,

"avgsvrttfb":<Double_value>,

"totsvrttlbtransactions":<Double_value>,
```

```
"surgecount":<Double_value>,

"httpmaxhdrszpkts":<Double_value>,

"primaryipaddress":<String_value>,

"maxclients":<Double_value>,

"requestbytesrate":<Double_value>,

"totalresponses":<Double_value>,

"totalresponsebytes":<Double_value>,

"httpmaxhdrfldlenpkts":<Double_value>,

"totalconnreassemblyqueue75":<Double_value>,

"toleratingttlbtransactions":<Double_value>,

"state":<String_value>,

"totalconnreassemblyqueueflush":<Double_value>,

"servicetype":<String_value>,

"curclntconnections":<Double_value>,

"responsebytesrate":<Double_value>,

"throughput":<Double_value>,

"vsvrservicehitsrate":<Double_value>,

"curload":<Double_value>,

"primaryport":<Integer_value>,

"throughputrate":<Double_value>,

"svrestablishedconn":<Double_value>,

"serviceorder":<Double_value>,
```

```
"requestsrate":<Double_value>,

"frustratingttlbtransactions":<Double_value>,

"totalrequestbytes":<Double_value>,

"responsesrate":<Double_value>,

"vsvrservicehits":<Double_value>,

"curreusepool":<Double_value>,

"totalrequests":<Double_value>,

"activetransactions":<Double_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/stat/service/ name_value><String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "service": [ {

"name":<String_value>,

"cursrvrconnections":<Double_value>,

"tcpmaxooopkts":<Double_value>,

"curtflags":<Double_value>,

"avgsvrttfb":<Double_value>,

"totsvrttlbtransactions":<Double_value>,

"surgecount":<Double_value>,

"httpmaxhdrszpkts":<Double_value>,

"primaryipaddress":<String_value>,

"maxclients":<Double_value>,

"requestbytesrate":<Double_value>,

"totalresponses":<Double_value>,

"totalresponsebytes":<Double_value>,

"httpmaxhdrfldlenpkts":<Double_value>,

"totalconnreassemblyqueue75":<Double_value>,

"toleratingttlbtransactions":<Double_value>,

"state":<String_value>,

"totalconnreassemblyqueueflush":<Double_value>,

"servicetype":<String_value>,

"curclntconnections":<Double_value>,

"responsebytesrate":<Double_value>,
```

```
"throughput":<Double_value>,

"vsvrservicehitsrate":<Double_value>,

"curload":<Double_value>,

"primaryport":<Integer_value>,

"throughputrate":<Double_value>,

"svrestablishedconn":<Double_value>,

"serviceorder":<Double_value>,

"requestsrate":<Double_value>,

"frustratingttlbtransactions":<Double_value>,

"totalrequestbytes":<Double_value>,

"responsesrate":<Double_value>,

"vsvrservicehits":<Double_value>,

"curreusepool":<Double_value>,

"totalrequests":<Double_value>,

"activetransactions":<Double_value>

}]}
```

servicegroup

Statistics for service group resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
servicegroupname	<String>	Read-write	Name of the service group for which to display settings. Minimum length = 1
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full
state	<String>	Read-only	Current state of the server. There are seven possible values: UP(7), DOWN(1), UNKNOWN(2), BUSY(3), OFS(Out of Service)(4), TROFS(Transition Out of Service)(5), TROFS_DOWN(Down When going Out of Service)(8)
servicetype	<String>	Read-only	The service type of this service.Possible values are ADNS, DNS, MYSQL, RTSP, SSL_DIAMETER, ADNS_TCP, DNS_TCP, NNTP, SIP_UDP, SSL_TCP, ANY, FTP, RADIUS, SNMP, TCP, DHCPRA, HTTP, RDP, SSL, TFTP, DIAMETER, MSSQL, RPCSVR, SSL_BRIDGE, UDP

Operations

(click to see Properties)

- GET (ALL)
- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/servicegroup **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/servicegroup? **args=servicegroupname: <String_value> ,detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get servicegroup resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/servicegroup? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "servicegroup": [ {

"servicegroupname":<String_value>,

"servicetype":<String_value>,

"state":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/stat/servicegroup/ servicegroupname_value><String>
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "servicegroup": [ {

"servicegroupname":<String_value>,

"servicetype":<String_value>,

"state":<String_value>

}]}
```

servicegroupmember

Statistics for service group entity resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
servicegroupname	<String>	Read-write	Displays statistics for the specified service group.Name of the service group. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			colon (:), at sign (@), equal sign (=), and hyphen (-) characters. CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my servicegroup" or 'my servicegroup'). Minimum length = 1
ip	<String>	Read-write	IP address of the service group. Mutually exclusive with the server name parameter.
servername	<String>	Read-write	Name of the server. Mutually exclusive with the IP address parameter. Minimum length = 1
port	<Integer>	Read-write	Port number of the service group member. Range 1 - 65535 * in CLI is represented as 65535 in NITRO API

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full
avgsvrttfb	<Double>	Read-only	Average TTFB between the Citrix ADC and the server. TTFB is the time interval between sending the request packet to a service and receiving the first response from the service
primaryipaddress	<String>	Read-only	The IP address on which the service is running.
primaryport	<Integer>	Read-only	The port on which the service is running.
servicetype	<String>	Read-only	The service type of this service.Possible values are ADNS, DNS, MYSQL, RTSP, SSL_DIAMETER, ADNS_TCP, DNS_TCP, NNTP, SIP_UDP, SSL_TCP, ANY, FTP, RADIUS, SNMP, TCP, DHCPRA, HTTP, RDP, SSL, TFTP, DIAMETER, MSSQL, RPCSVR, SSL_BRIDGE, UDP

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
state	<String>	Read-only	Current state of the server. There are seven possible values: UP(7), DOWN(1), UNKNOWN(2), BUSY(3), OFS(Out of Service)(4), TROFS(Transition Out of Service)(5), TROFS_DOWN(Down When going Out of Service)(8)
svcgrpmemberbindingorder	<Double>	Read-only	Order with which service group member is bound to service group
totalrequests	<Double>	Read-only	Total number of requests received on this service or virtual server. (This applies to HTTP/SSL services and servers.)
requestsrate	<Double>	Read-only	Rate (/s) counter for totalrequests
totalresponses	<Double>	Read-only	Number of responses received on this service or virtual server. (This applies to HTTP/SSL services and servers.)
responsesrate	<Double>	Read-only	Rate (/s) counter for totalresponses

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
totalrequestbytes	<Double>	Read-only	Total number of request bytes received on this service or virtual server.
requestbytesrate	<Double>	Read-only	Rate (/s) counter for totalrequestbytes
totalresponsebytes	<Double>	Read-only	Number of response bytes received by this service or virtual server.
responsebytesrate	<Double>	Read-only	Rate (/s) counter for totalresponsebytes
curclntconnections	<Double>	Read-only	Number of current client connections.
surgecount	<Double>	Read-only	Number of requests in the surge queue.
cursrvrconnections	<Double>	Read-only	Number of current connections to the actual servers behind the virtual server.
svrestablishedconn	<Double>	Read-only	Number of server connections in ESTABLISHED state.
curreusepool	<Double>	Read-only	Number of requests in the idle queue/ reuse pool.
maxclients	<Double>	Read-only	Maximum open connections allowed on this service.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
totalconnreassemblyqueue75	<Double>	Read-only	Total no of connections with 75% TCP reassembly queue
totalconnreassemblyqueueflush	<Double>	Read-only	Total no of connections incurred TCP reassembly queue flush
totsvrttlbtransactions	<Double>	Read-only	Total transactions where server TTLB is calculated.
toleratingttlbtransactions	<Double>	Read-only	Tolerable transactions based on APDEX threshold (>T ;; <4T).
frustratingttlbtransactions	<Double>	Read-only	Frustrating transactions based on APDEX threshold (>4T).
curload	<Double>	Read-only	Load on the service that is calculated from the bound load based monitor.
httpmaxhdrszpkts	<Double>	Read-only	Number of http max header size packet parsing failures
httpmaxhdrfldlenpkts	<Double>	Read-only	Number of HTTP requests exceeding max header field length
tcpmaxooopkts	<Double>	Read-only	No of times max out of order packets reached

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
serviceorder	<Double>	Read-only	Order with which service is bound to vserver

Operations

(click to see Properties)

- GET (ALL)
- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/servicegroupmember **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/servicegroupmember? **args= servicegroupname:<String_value>, ip: <String_value> ,servername: <String_value> ,port: <Integer_value> ,detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get servicegroupmember resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/servicegroupmember? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "servicegroupmember": [ {

"servicegroupname":<String_value>,

"avgsvrttfb":<Double_value>,

"tcpmaxooopkts":<Double_value>,

"cursrvrconnections":<Double_value>,

"surgecount":<Double_value>,
```

```
"totsvrttlbtransactions":<Double_value>,

"svcgrpmemberbindingorder":<Double_value>,

"maxclients":<Double_value>,

"primaryipaddress":<String_value>,

"httpmaxhdrszpkts":<Double_value>,

"totalresponsebytes":<Double_value>,

"totalresponses":<Double_value>,

"requestbytesrate":<Double_value>,

"totalconnreassemblyqueue75":<Double_value>,

"httpmaxhdrfldlenpkts":<Double_value>,

"state":<String_value>,

"toleratingttlbtransactions":<Double_value>,

"curclntconnections":<Double_value>,

"responsebytesrate":<Double_value>,

"servicetype":<String_value>,

"totalconnreassemblyqueueflush":<Double_value>,

"serviceorder":<Double_value>,

"svrestablishedconn":<Double_value>,

"primaryport":<Integer_value>,

"curload":<Double_value>,

"requestsrate":<Double_value>,

"frustratingttlbtransactions":<Double_value>,
```

```
"totalrequestbytes":<Double_value>,

"responsesrate":<Double_value>,

"totalrequests":<Double_value>,

"curreusepool":<Double_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/stat/servicegroupmember/ servicegroupname_value><String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "servicegroupmember": [ {

"servicegroupname":<String_value>,

"avgsvrttfb":<Double_value>,

"tcpmaxooopkts":<Double_value>,

"cursrvrconnections":<Double_value>,

"surgecount":<Double_value>,
```

```
"totsvrttlbtransactions":<Double_value>,

"svcgrpmemberbindingorder":<Double_value>,

"maxclients":<Double_value>,

"primaryipaddress":<String_value>,

"httpmaxhdrszpkts":<Double_value>,

"totalresponsebytes":<Double_value>,

"totalresponses":<Double_value>,

"requestbytesrate":<Double_value>,

"totalconnreassemblyqueue75":<Double_value>,

"httpmaxhdrfldlenpkts":<Double_value>,

"state":<String_value>,

"toleratingttlbtransactions":<Double_value>,

"curclntconnections":<Double_value>,

"responsebytesrate":<Double_value>,

"servicetype":<String_value>,

"totalconnreassemblyqueueflush":<Double_value>,

"serviceorder":<Double_value>,

"svrestablishedconn":<Double_value>,

"primaryport":<Integer_value>,

"curload":<Double_value>,

"requestsrate":<Double_value>,

"frustratingttlbtransactions":<Double_value>,
```

```
"totalrequestbytes":<Double_value>,

"responsesrate":<Double_value>,

"totalrequests":<Double_value>,

"curreusepool":<Double_value>

}]}
```

bot

Bot

Bot Management.

NAME	DESCRIPTION
bot	Statistics for bot.
botpolicy	Statistics for Bot policy resource.
botpolicylabel	Statistics for Bot policy label resource.
botprofile	Statistics for Bot profile resource.

bot

Statistics for bot.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
clearstats	<String>	Read-write	Clear the statsistics / counters.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = basic, full
botrequests	<Double>	Read-only	HTTP/HTTPS requests sent to your protected web servers via the Bot Management.
botrequestsrate	<Double>	Read-only	Rate (/s) counter for botrequests
botreqbytes	<Double>	Read-only	Number of bytes transfered for requests
botreqbytesrate	<Double>	Read-only	Rate (/s) counter for botreqbytes
botresponses	<Double>	Read-only	HTTP/HTTPS responses sent by your protected web servers via the Bot Management.
botresponsesrate	<Double>	Read-only	Rate (/s) counter for botresponses
botresbytes	<Double>	Read-only	Number of bytes transfered for responses
botresbytesrate	<Double>	Read-only	Rate (/s) counter for botresbytes
bottotallog	<Double>	Read-only	Total number of logs by the bot management.
botlograte	<Double>	Read-only	Rate (/s) counter for bottotallog

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
bottotaldrop	<Double>	Read-only	Total number of drops by the bot management.
botdroprate	<Double>	Read-only	Rate (/s) counter for bottotaldrop
bottotalredirect	<Double>	Read-only	Total number of redirects by the bot management.
botredirectrate	<Double>	Read-only	Rate (/s) counter for bottotalredirect
bottotalreset	<Double>	Read-only	Total number of resets by the bot management.
botresetrate	<Double>	Read-only	Rate (/s) counter for bottotalreset
botvioldevicefingerprint	<Double>	Read-only	Number of device fingerprint violations seen by the Bot Management.
botvioldevicefingerprintrate	<Double>	Read-only	Rate (/s) counter for botvioldevicefingerprint
botvioldevicefingerprintlog	<Double>	Read-only	Number of device fingerprint violations logged by the Bot Management.
botvioldevicefingerprintlograte	<Double>	Read-only	Rate (/s) counter for botvioldevicefingerprintlog
botvioldevicefingerprintdrop	<Double>	Read-only	Number of device fingerprint violations

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			dropped by the Bot Management.
botvioldevicefingerprintdroprate	<Double>	Read-only	Rate (/s) counter for botvioldevicefingerprintdrop
botvioldevicefingerprintredirect	<Double>	Read-only	Number of device fingerprint violations requests redirected by the Bot Management to a different Web page or web server.
botvioldevicefingerprintredirectrate	<Double>	Read-only	Rate (/s) counter for botvioldevicefingerprintredirect
botvioldevicefingerprintcaptcha	<Double>	Read-only	Number of device fingerprint violations requests for which CAPTCHA challenge was sent.
botvioldevicefingerprintcaptcharate	<Double>	Read-only	Rate (/s) counter for botvioldevicefingerprintcaptcha
botvioldevicefingerprintreset	<Double>	Read-only	Number of device fingerprint violations reset by the Bot Management.
botvioldevicefingerprintresetrate	<Double>	Read-only	Rate (/s) counter for botvioldevicefingerprintreset
botviolipreputation	<Double>	Read-only	Number of ip reputation violations

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			seen by the Bot Management.
botviolipreputationrate	<Double>	Read-only	Rate (/s) counter for botviolipreputation
botviolipreputationlog	<Double>	Read-only	Number of ip reputation violations logged by the Bot Management.
botviolipreputationlograte	<Double>	Read-only	Rate (/s) counter for botviolipreputationlog
botviolipreputationdrop	<Double>	Read-only	Number of ip reputation violations dropped by the Bot Management.
botviolipreputationdroprate	<Double>	Read-only	Rate (/s) counter for botviolipreputationdrop
botviolipreputationredirect	<Double>	Read-only	Number of ip reputation violations requests redirected by the Bot Management to a different Web page or web server.
botviolipreputationredirectrate	<Double>	Read-only	Rate (/s) counter for botviolipreputationredirect
botviolipreputationcaptcha	<Double>	Read-only	Number of ip reputation violations requests for which CAPTCHA challenge was sent.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
botviolipreputationcaptcharate	<Double>	Read-only	Rate (/s) counter for botviolipreputationcaptcha
botviolipreputationreset	<Double>	Read-only	Number of ip reputation violations reset by the Bot Management.
botviolipreputationresetrate	<Double>	Read-only	Rate (/s) counter for botviolipreputationreset
botviolwhitelist	<Double>	Read-only	Number of white list violations seen by the Bot Management.
botviolwhitelistrate	<Double>	Read-only	Rate (/s) counter for botviolwhitelist
botviolwhitelistlog	<Double>	Read-only	Number of white list violations logged by the Bot Management.
botviolwhitelistlograte	<Double>	Read-only	Rate (/s) counter for botviolwhitelistlog
botviolblacklist	<Double>	Read-only	Number of black list violations seen by the Bot Management.
botviolblacklistrate	<Double>	Read-only	Rate (/s) counter for botviolblacklist
botviolblacklistlog	<Double>	Read-only	Number of black list violations logged by the Bot Management.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
botviolblacklistlograte	<Double>	Read-only	Rate (/s) counter for botviolblacklistlog
botviolblacklistdrop	<Double>	Read-only	Number of black list violations dropped by the Bot Management.
botviolblacklistdroprate	<Double>	Read-only	Rate (/s) counter for botviolblacklistdrop
botviolblacklistreset	<Double>	Read-only	Number of black list violations reset by the Bot Management.
botviolblacklistresetrate	<Double>	Read-only	Rate (/s) counter for botviolblacklistreset
botviolblacklistredirect	<Double>	Read-only	Number of black list violations redirected by the Bot Management to a different Web page or web server.
botviolblacklistredirectrate	<Double>	Read-only	Rate (/s) counter for botviolblacklistredirect
botviolratelimit	<Double>	Read-only	Number of rate limiting violations seen by the Bot Management.
botviolratelimitrate	<Double>	Read-only	Rate (/s) counter for botviolratelimit
botviolratelimitlog	<Double>	Read-only	Number of rate limiting violations

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			logged by the Bot Management.
botviolratelimitlograte	<Double>	Read-only	Rate (/s) counter for botviolratelimitlog
botviolratelimitdrop	<Double>	Read-only	Number of rate limiting violations dropped by the Bot Management.
botviolratelimitdroprate	<Double>	Read-only	Rate (/s) counter for botviolratelimitdrop
botviolratelimitredirect	<Double>	Read-only	Number of rate limiting violations requests redirected by the Bot Management to a different Web page or web server.
botviolratelimitredirectrate	<Double>	Read-only	Rate (/s) counter for botviolratelimitredirect
botviolratelimitexceedresponse	<Double>	Read-only	Number of rate limiting violations requests resulted in too many requests response by the Bot Management.
botviolratelimitexceedresponserate	<Double>	Read-only	Rate (/s) counter for botviolratelimitexceedresponse
botviolratelimitreset	<Double>	Read-only	Number of rate limiting violations reset by the Bot Management.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
botviolratelimitresetrate	<Double>	Read-only	Rate (/s) counter for botviolratelimitreset
botviolstaticsignature	<Double>	Read-only	Number of static signature violations seen by the Bot Management.
botviolstaticsignature rate	<Double>	Read-only	Rate (/s) counter for botviolstaticsignature
botviolstaticsignature log	<Double>	Read-only	Number of static signature violations logged by the Bot Management.
botviolstaticsignature lograte	<Double>	Read-only	Rate (/s) counter for botviolstaticsignature log
botviolstaticsignature drop	<Double>	Read-only	Number of static signature violations dropped by the Bot Management.
botviolstaticsignature droprate	<Double>	Read-only	Rate (/s) counter for botviolstaticsignature drop
botviolstaticsignature redirect	<Double>	Read-only	Number of static signature violations requests redirected by the Bot Management to a different Web page or web server.
botviolstaticsignature redirectrate	<Double>	Read-only	Rate (/s) counter for botviolstaticsignature redirect

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
botviolstaticsignature reset	<Double>	Read-only	Number of static signature violations requests reset by the Bot Management to a different Web page or web server.
botviolstaticsignature resetrate	<Double>	Read-only	Rate (/s) counter for botviolstaticsignature reset
botvioltps	<Double>	Read-only	Number of tps violations seen by the Bot Management.
botvioltpsrate	<Double>	Read-only	Rate (/s) counter for botvioltps
botvioltpslog	<Double>	Read-only	Number of tps violations logged by the Bot Management.
botvioltpslograte	<Double>	Read-only	Rate (/s) counter for botvioltpslog
botvioltpsdrop	<Double>	Read-only	Number of tps violations dropped by the Bot Management.
botvioltpsdroprate	<Double>	Read-only	Rate (/s) counter for botvioltpsdrop
botvioltpsredirect	<Double>	Read-only	Number of tps violations requests redirected by the Bot Management to a different Web page or web server.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
botvioltpsredirectrate	<Double>	Read-only	Rate (/s) counter for botvioltpsredirect
botvioltpsreset	<Double>	Read-only	Number of tps violations reset by the Bot Management.
botvioltpsresetrate	<Double>	Read-only	Rate (/s) counter for botvioltpsreset
botvioltpscaptcha	<Double>	Read-only	Number of TPS violations requests for which CAPTCHA challenge was sent.
botvioltpscaptcharate	<Double>	Read-only	Rate (/s) counter for botvioltpscaptcha
botviolcaptcha	<Double>	Read-only	Number of Captcha challenge failures seen by the Bot Management.
botviolcaptcharate	<Double>	Read-only	Rate (/s) counter for botviolcaptcha
botviolcaptchalog	<Double>	Read-only	Number of Captcha challenge failures logged by the Bot Management.
botviolcaptchalograte	<Double>	Read-only	Rate (/s) counter for botviolcaptchalog
botviolcaptchadrop	<Double>	Read-only	Number of Captcha challenge failures dropped by the Bot Management.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
botviolcaptchadroprate	<Double>	Read-only	Rate (/s) counter for botviolcaptchadrop
botviolcaptcharedirect	<Double>	Read-only	Number of Captcha challenge failures redirected by the Bot Management.
botviolcaptcharedirectrate	<Double>	Read-only	Rate (/s) counter for botviolcaptcharedirect
botviolcaptchareset	<Double>	Read-only	Number of Captcha challenge failures reset by the Bot Management.
botviolcaptcharesetrate	<Double>	Read-only	Rate (/s) counter for botviolcaptchareset
botvioltrap	<Double>	Read-only	Number of trap violations seen by the Bot Management.
botvioltraprate	<Double>	Read-only	Rate (/s) counter for botvioltrap
botvioltraplog	<Double>	Read-only	Number of trap violations logged by the Bot Management.
botvioltraplograte	<Double>	Read-only	Rate (/s) counter for botvioltraplog
botvioltrapdrop	<Double>	Read-only	Number of trap violations dropped by the Bot Management.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
botvioltrapdroprate	<Double>	Read-only	Rate (/s) counter for botvioltrapdrop
botvioltrapredirect	<Double>	Read-only	Number of trap violations requests redirected by the Bot Management to a different Web page or web server.
botvioltrapredirectrate	<Double>	Read-only	Rate (/s) counter for botvioltrapredirect
botvioltrapreset	<Double>	Read-only	Number of trap violations reset by the Bot Management.
botvioltrapresetrate	<Double>	Read-only	Rate (/s) counter for botvioltrapreset
botcfgwhitelist	<Double>	Read-only	Profiles with Whitelist enabled.
botcfgblacklist	<Double>	Read-only	Profiles with Blacklist enabled.
botcfgiprep	<Double>	Read-only	Profiles with IP Reputation enabled.
botcfgratelimit	<Double>	Read-only	Profiles with Ratelimit enabled.
botcfgsignature	<Double>	Read-only	Profiles with Static Signatures enabled.
botcfgdfp	<Double>	Read-only	Profiles with Device Fingerprint enabled.
botcfgtps	<Double>	Read-only	Profiles with TPS enabled.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
botcfgtrap	<Double>	Read-only	Profiles with Bot Trap enabled.
botcfgkmdetection	<Double>	Read-only	Profiles with Keyboard mouse detection enabled.

Operations

(click to see Properties)

- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/bot **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/bot? **args=detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get bot resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/bot? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "bot": [ {

"botvioltpsdroprate":<Double_value>,

"botrequests":<Double_value>,

"botvioldevicefingerprintrate":<Double_value>,

"botvioldevicefingerprintredirect":<Double_value>,

"botviolipreputationcaptcha":<Double_value>,

"botvioldevicefingerprintdrop":<Double_value>,
```

```
"botviolblacklistlograte":<Double_value>,

"botviolipreputation":<Double_value>,

"botviolblacklist":<Double_value>,

"botviolblacklistdrop":<Double_value>,

"botvioltpsrate":<Double_value>,

"botvioldevicefingerprintresetrate":<Double_value>,

"botviolblacklistrate":<Double_value>,

"botviolstaticsignaturereset":<Double_value>,

"botviolstaticsignaturedroprate":<Double_value>,

"botvioltrapreset":<Double_value>,

"botvioldevicefingerprintlog":<Double_value>,

"botcfgtps":<Double_value>,

"botviolblacklistresetrate":<Double_value>,

"botviolipreputationredirectrate":<Double_value>,

"botvioltrapresetrate":<Double_value>,

"botviolblacklistdroprate":<Double_value>,

"botcfgblacklist":<Double_value>,

"botvioltpsresetrate":<Double_value>,

"botresbytes":<Double_value>,

"botcfgsignature":<Double_value>,

"botviolcaptcharate":<Double_value>,

"botvioldevicefingerprintreset":<Double_value>,
```

```
"botviolcaptchadroprate":<Double_value>,

"botviolipreputationlograte":<Double_value>,

"botviolratelimitdroprate":<Double_value>,

"botvioltrapredirectrate":<Double_value>,

"botvioltpslog":<Double_value>,

"botviolcaptcharedirect":<Double_value>,

"botvioltrapdroprate":<Double_value>,

"botvioltrap":<Double_value>,

"botviolipreputationresetrate":<Double_value>,

"botreqbytesrate":<Double_value>,

"botviolcaptcha":<Double_value>,

"botlograte":<Double_value>,

"botvioltpsredirectrate":<Double_value>,

"botviolipreputationreset":<Double_value>,

"botvioltpsdrop":<Double_value>,

"botviolstaticsignatureredirectrate":<Double_value>,

"botviolwhitelist":<Double_value>,

"botviolwhitelistlograte":<Double_value>,

"bottotalreset":<Double_value>,

"botviolwhitelistrate":<Double_value>,

"botviolipreputationlog":<Double_value>,

"botviolcaptcharedirectrate":<Double_value>,
```

```
"botviolipreputationcaptcharate":<Double_value>,

"botcfgdfp":<Double_value>,

"botviolblacklistredirectrate":<Double_value>,

"botviolratelimitrate":<Double_value>,

"botviolratelimitdrop":<Double_value>,

"botviolcaptchareset":<Double_value>,

"botviolratelimitlograte":<Double_value>,

"botviolratelimit":<Double_value>,

"botviolcaptchalograte":<Double_value>,

"botviolblacklistredirect":<Double_value>,

"bottotallog":<Double_value>,

"botresponsesrate":<Double_value>,

"botviolratelimitexceededresponse":<Double_value>,

"botvioltpslograte":<Double_value>,

"botviolstaticsignature":<Double_value>,

"botcfgtrap":<Double_value>,

"botvioltpscaptcharate":<Double_value>,

"botviolstaticsignaturelog":<Double_value>,

"botviolratelimitredirectrate":<Double_value>,

"botvioltpsreset":<Double_value>,

"botviolratelimitresetrate":<Double_value>,

"botvioltrapredirect":<Double_value>,
```

```
"botdroprate":<Double_value>,

"botviolratelimitlog":<Double_value>,

"botviolstaticsignaturerate":<Double_value>,

"botviolcaptcharesetrate":<Double_value>,

"botviolblacklistreset":<Double_value>,

"botvioliprepuationredirect":<Double_value>,

"botvioldevicefingerprint":<Double_value>,

"botvioldevicefingerprintdroprate":<Double_value>,

"botviolstaticsignaturedrop":<Double_value>,

"botreqbytes":<Double_value>,

"botviolstaticsignaturelograte":<Double_value>,

"botcfgwhitelist":<Double_value>,

"botcfgiprep":<Double_value>,

"botvioldevicefingerprintredirectrate":<Double_value>,

"botvioltraplog":<Double_value>,

"botvioltraprate":<Double_value>,

"botvioldevicefingerprintlograte":<Double_value>,

"botviolstaticsignatureresetrate":<Double_value>,

"botviolwhitelistlog":<Double_value>,

"botvioldevicefingerprintcaptcharate":<Double_value>,

"botvioltpscaptcha":<Double_value>,

"botviolstaticsignatureredirect":<Double_value>,
```

```
"botviolcaptchadrop":<Double_value>,

"botviolratelimitreset":<Double_value>,

"botviolipreputationrate":<Double_value>,

"botviolblacklistlog":<Double_value>,

"botredirectrate":<Double_value>,

"botcfgkmdetection":<Double_value>,

"bottotaldrop":<Double_value>,

"botviolcaptchalog":<Double_value>,

"botcfgratelimit":<Double_value>,

"botresponses":<Double_value>,

"botvioltpsredirect":<Double_value>,

"botviolipreputationdrop":<Double_value>,

"botvioltraplograte":<Double_value>,

"botresbytesrate":<Double_value>,

"botresetrate":<Double_value>,

"botviolratelimitredirect":<Double_value>,

"botvioltrapdrop":<Double_value>,

"botvioltps":<Double_value>,

"botrequestsrate":<Double_value>,

"botviolratelimitexceededresponserate":<Double_value>,

"botvioldevicefingerprintcaptcha":<Double_value>,

"bottotalredirect":<Double_value>,
```

```
"botviolipreputationdroprate":<Double_value>

}]}
```

botpolicy

Statistics for Bot policy resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the bot policy for which to show detailed statistics. Minimum length = 1
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full
pipolicyhits	<Double>	Read-only	Number of hits on the policy
pipolicyhitsrate	<Double>	Read-only	Rate (/s) counter for pipolicyhits
pipolicyundefhits	<Double>	Read-only	Number of undef hits on the policy
pipolicyundefhitsrate	<Double>	Read-only	Rate (/s) counter for pipolicyundefhits

Operations

(click to see Properties)

- GET (ALL)

- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/botpolicy **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/botpolicy? **args=name: <String_value> ,detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get botpolicy resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/botpolicy? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "botpolicy": [ {

"name":<String_value>,

"pipolicyundefhitsrate":<Double_value>,

"pipolicyhitsrate":<Double_value>,

"pipolicyundefhits":<Double_value>,

"pipolicyhits":<Double_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/stat/botpolicy/ name_value><String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "botpolicy": [ {

"name":<String_value>,

"pipolicyundefhitsrate":<Double_value>,

"pipolicyhitsrate":<Double_value>,

"pipolicyundefhits":<Double_value>,

"pipolicyhits":<Double_value>

}]}
```

botpolicylabel

Statistics for Bot policy label resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
labelname	<String>	Read-write	Name of the bot policy label. Minimum length = 1
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
pipolicylabelhits	<Double>	Read-only	Number of times policy label was invoked.
pipolicylabelhitsrate	<Double>	Read-only	Rate (/s) counter for pipolicylabelhits

Operations

(click to see Properties)

- GET (ALL)
- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/botpolicylabel **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/botpolicylabel? **args=labelname: <String_value> ,detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get botpolicylabel resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/botpolicylabel? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "botpolicylabel": [ {

"labelname":<String_value>,

"pipolicylabelhitsrate":<Double_value>,

"pipolicylabelhits":<Double_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/stat/botpolicylabel/ labelname_value><String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "botpolicylabel": [ {

"labelname":<String_value>,

"pipolicylabelhitsrate":<Double_value>,

"pipolicylabelhits":<Double_value>

}]}
```

botprofile

Statistics for Bot profile resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the bot profile.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum length = 1 Maximum length = 31
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full
botrequestsperprofile	<Double>	Read-only	HTTP/HTTPS requests sent to your protected web servers via the Bot profile.
botrequestsperprofile rate	<Double>	Read-only	Rate (/s) counter for botrequestsperprofile
botreqbytesperprofile	<Double>	Read-only	Number of bytes transfered for requests
botreqbytesperprofile rate	<Double>	Read-only	Rate (/s) counter for botreqbytesperprofile
botresponsesperprofi le	<Double>	Read-only	HTTP/HTTPS responses sent by your protected web servers via the Bot profile.
botresponsesperprofi lerate	<Double>	Read-only	Rate (/s) counter for botresponsesperprofi le
botresbytesperprofile	<Double>	Read-only	Number of bytes transfered for responses

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
botresbytesperprofilerate	<Double>	Read-only	Rate (/s) counter for botresbytesperprofile
bottotallogprofile	<Double>	Read-only	Total number of logs by the Bot profile.
botlogprofilerate	<Double>	Read-only	Rate (/s) counter for bottotallogprofile
bottotaldropprofile	<Double>	Read-only	Total number of drops by the Bot profile.
botdropprofilerate	<Double>	Read-only	Rate (/s) counter for bottotaldropprofile
bottotalredirectprofile	<Double>	Read-only	Total number of redirects by the Bot profile.
botredirectprofilerate	<Double>	Read-only	Rate (/s) counter for bottotalredirectprofile
bottotalresetprofile	<Double>	Read-only	Total number of resets by the Bot profile.
botresetprofilerate	<Double>	Read-only	Rate (/s) counter for bottotalresetprofile
botvioldevicefingerprintprofile	<Double>	Read-only	Number of device fingerprint violations seen by the Bot profile.
botvioldevicefingerprintprofilerate	<Double>	Read-only	Rate (/s) counter for botvioldevicefingerprintprofile
botvioldevicefingerprintlogprofile	<Double>	Read-only	Number of device fingerprint violations

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			logged by the Bot profile.
botvioldevicefingerprintlogprofilerate	<Double>	Read-only	Rate (/s) counter for botvioldevicefingerprintlogprofile
botvioldevicefingerprintdropprofile	<Double>	Read-only	Number of device fingerprint violations dropped by the Bot profile.
botvioldevicefingerprintdropprofilerate	<Double>	Read-only	Rate (/s) counter for botvioldevicefingerprintdropprofile
botvioldevicefingerprintredirectprofile	<Double>	Read-only	Number of device fingerprint violations requests redirected by the Bot profile to a different Web page or web server.
botvioldevicefingerprintredirectprofilerate	<Double>	Read-only	Rate (/s) counter for botvioldevicefingerprintredirectprofile
botvioldevicefingerprintcaptchaprofile	<Double>	Read-only	Number of device fingerprint violation requests for which CAPTCHA challenge was sent due to Bot profile.
botvioldevicefingerprintcaptchaprofilerate	<Double>	Read-only	Rate (/s) counter for botvioldevicefingerprintcaptchaprofile
botvioldevicefingerprintresetprofile	<Double>	Read-only	Number of device fingerprint violations

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			reset by the Bot profile.
botvioldevicefingerprintresetprofilerate	<Double>	Read-only	Rate (/s) counter for botvioldevicefingerprintresetprofile
botviolipreputationprofile	<Double>	Read-only	Number of ip reputation violations seen by the Bot profile.
botviolipreputationprofilerate	<Double>	Read-only	Rate (/s) counter for botviolipreputationprofile
botviolipreputationlogprofile	<Double>	Read-only	Number of ip reputation violations logged by the Bot Profile.
botviolipreputationlogprofilerate	<Double>	Read-only	Rate (/s) counter for botviolipreputationlogprofile
botviolipreputationdropprofile	<Double>	Read-only	Number of ip reputation violations dropped by the Bot profile.
botviolipreputationdropprofilerate	<Double>	Read-only	Rate (/s) counter for botviolipreputationdropprofile
botviolipreputationredirectprofile	<Double>	Read-only	Number of ip reputation violations requests redirected by the Bot profile to a different Web page or web server.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
botviolipreputationredirectprofilerate	<Double>	Read-only	Rate (/s) counter for botviolipreputationredirectprofile
botviolipreputationcaptchaprofile	<Double>	Read-only	Number of ip reputation violation requests for which CAPTCHA challenge was sent due to Bot profile.
botviolipreputationcaptchaprofilerate	<Double>	Read-only	Rate (/s) counter for botviolipreputationcaptchaprofile
botviolipreputationresetprofile	<Double>	Read-only	Number of ip reputation violations reset by the Bot profile.
botviolipreputationresetprofilerate	<Double>	Read-only	Rate (/s) counter for botviolipreputationresetprofile
botviolwhitelistprofile	<Double>	Read-only	Number of white list violations seen by the Bot profile.
botviolwhitelistprofilerate	<Double>	Read-only	Rate (/s) counter for botviolwhitelistprofile
botviolwhitelistlogprofile	<Double>	Read-only	Number of white list violations logged by the Bot profile.
botviolwhitelistlogprofilerate	<Double>	Read-only	Rate (/s) counter for botviolwhitelistlogprofile

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
botviolblacklistprofile	<Double>	Read-only	Number of black list violations seen by the Bot profile.
botviolblacklistprofile rate	<Double>	Read-only	Rate (/s) counter for botviolblacklistprofile
botviolblacklistlogpro file	<Double>	Read-only	Number of black list violations logged by the Bot profile.
botviolblacklistlogpro filerate	<Double>	Read-only	Rate (/s) counter for botviolblacklistlogpro file
botviolblacklistdroppr ofile	<Double>	Read-only	Number of black list violations dropped by the Bot profile.
botviolblacklistdroppr ofilerate	<Double>	Read-only	Rate (/s) counter for botviolblacklistdroppr ofile
botviolblacklistresetp rofile	<Double>	Read-only	Number of black list violations reset by the Bot profile.
botviolblacklistresetp rofilerate	<Double>	Read-only	Rate (/s) counter for botviolblacklistresetp rofile
botviolblacklistredire ctprofile	<Double>	Read-only	Number of black list violations redirected by the Bot profile to a different Web page or web server.
botviolblacklistredire ctprofilerate	<Double>	Read-only	Rate (/s) counter for botviolblacklistredire ctprofile

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
botviolratelimitprofile	<Double>	Read-only	Number of rate limiting violations seen by the Bot profile.
botviolratelimitprofilerate	<Double>	Read-only	Rate (/s) counter for botviolratelimitprofile
botviolratelimitlogprofile	<Double>	Read-only	Number of rate limiting violations logged by the Bot profile.
botviolratelimitlogprofilerate	<Double>	Read-only	Rate (/s) counter for botviolratelimitlogprofile
botviolratelimitdropprofile	<Double>	Read-only	Number of rate limiting violations dropped by the Bot profile.
botviolratelimitdropprofilerate	<Double>	Read-only	Rate (/s) counter for botviolratelimitdropprofile
botviolratelimitredirectprofile	<Double>	Read-only	Number of rate limiting violations requests redirected by the Bot profile to a different Web page or web server.
botviolratelimitredirectprofilerate	<Double>	Read-only	Rate (/s) counter for botviolratelimitredirectprofile
botviolratelimitexceedresponseprofile	<Double>	Read-only	Number of rate limiting violations requests responded resulted in too many

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			requests response by the Bot profile.
botviolratelimitexceedresponseprofilerate	<Double>	Read-only	Rate (/s) counter for botviolratelimitexceedresponseprofile
botviolratelimitresetprofile	<Double>	Read-only	Number of rate limiting violations reset by the Bot profile.
botviolratelimitresetprofilerate	<Double>	Read-only	Rate (/s) counter for botviolratelimitresetprofile
botviolstaticsignature profile	<Double>	Read-only	Number of static signatutre violations seen by the Bot profile.
botviolstaticsignature profilerate	<Double>	Read-only	Rate (/s) counter for botviolstaticsignature profile
botviolstaticsignature logprofile	<Double>	Read-only	Number of static signatutre violations logged by the Bot profile.
botviolstaticsignature logprofilerate	<Double>	Read-only	Rate (/s) counter for botviolstaticsignature logprofile
botviolstaticsignature dropprofile	<Double>	Read-only	Number of static signatutre violations dropped by the Bot profile.
botviolstaticsignature dropprofilerate	<Double>	Read-only	Rate (/s) counter for botviolstaticsignature dropprofile

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
botviolstaticsignature redirectprofile	<Double>	Read-only	Number of static signatutre violations redirected by the Bot profile to a different Web page or web server.
botviolstaticsignature redirectprofilerate	<Double>	Read-only	Rate (/s) counter for botviolstaticsignature redirectprofile
botviolstaticsignature resetprofile	<Double>	Read-only	Number of static signatutre violations reset by the Bot profile to a different Web page or web server.
botviolstaticsignature resetprofilerate	<Double>	Read-only	Rate (/s) counter for botviolstaticsignature resetprofile
botvioltpsprofile	<Double>	Read-only	Number of tps violations seen by the Bot profile.
botvioltpsprofilerate	<Double>	Read-only	Rate (/s) counter for botvioltpsprofile
botvioltpslogprofile	<Double>	Read-only	Number of tps violations logged by the Bot profile.
botvioltpslogprofilerate	<Double>	Read-only	Rate (/s) counter for botvioltpslogprofile
botvioltpsdropprofile	<Double>	Read-only	Number of tps violations dropped by the Bot profile.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
botvioltpsdropprofilerate	<Double>	Read-only	Rate (/s) counter for botvioltpsdropprofile
botvioltpsredirectprofile	<Double>	Read-only	Number of tps violations requests redirected by the Bot profile to a different Web page or web server.
botvioltpsredirectprofilerate	<Double>	Read-only	Rate (/s) counter for botvioltpsredirectprofile
botvioltpsresetprofile	<Double>	Read-only	Number of tps violations reset by the Bot profile.
botvioltpsresetprofilerate	<Double>	Read-only	Rate (/s) counter for botvioltpsresetprofile
botvioltpscaptchaprofile	<Double>	Read-only	Number of tps violation requests for which CAPTCHA challenge was sent due to Bot profile.
botvioltpscaptchaprofilerate	<Double>	Read-only	Rate (/s) counter for botvioltpscaptchaprofile
botviolcaptchaprofile	<Double>	Read-only	Number of Captcha challenge failures seen by the Bot profile.
botviolcaptchaprofilerate	<Double>	Read-only	Rate (/s) counter for botviolcaptchaprofile
botviolcaptchalogprofile	<Double>	Read-only	Number of Captcha challenge failures

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			logged by the Bot profile.
botviolcaptchalogprofilerate	<Double>	Read-only	Rate (/s) counter for botviolcaptchalogprofile
botviolcaptchadropprofile	<Double>	Read-only	Number of Captcha challenge failures dropped by the Bot profile.
botviolcaptchadropprofilerate	<Double>	Read-only	Rate (/s) counter for botviolcaptchadropprofile
botviolcaptcharedirectprofile	<Double>	Read-only	Number of Captcha challenge failures redirected by the Bot profile.
botviolcaptcharedirectprofilerate	<Double>	Read-only	Rate (/s) counter for botviolcaptcharedirectprofile
botviolcaptcharesetprofile	<Double>	Read-only	Number of Captcha challenge failures reset by the Bot profile.
botviolcaptcharesetprofilerate	<Double>	Read-only	Rate (/s) counter for botviolcaptcharesetprofile
botvioltrapprofile	<Double>	Read-only	Number of trap violations seen by the Bot profile.
botvioltrapprofilerate	<Double>	Read-only	Rate (/s) counter for botvioltrapprofile

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
botvioltraplogprofile	<Double>	Read-only	Number of trap violations logged by the Bot profile.
botvioltraplogprofilerate	<Double>	Read-only	Rate (/s) counter for botvioltraplogprofile
botvioltrapdropprofile	<Double>	Read-only	Number of trap violations dropped by the Bot profile.
botvioltrapdropprofilerate	<Double>	Read-only	Rate (/s) counter for botvioltrapdropprofile
botvioltrapredirectprofile	<Double>	Read-only	Number of trap violations requests redirected by the Bot profile to a different Web page or web server.
botvioltrapredirectprofilerate	<Double>	Read-only	Rate (/s) counter for botvioltrapredirectprofile
botvioltrapresetprofile	<Double>	Read-only	Number of trap violations reset by the Bot profile.
botvioltrapresetprofilerate	<Double>	Read-only	Rate (/s) counter for botvioltrapresetprofile
botcfgwhitelistprofile	<Double>	Read-only	Whitelist enabled under bot profile.
botcfgblacklistprofile	<Double>	Read-only	Blacklist enabled under bot profile.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
botcfgiprepprofile	<Double>	Read-only	IP Reputation enabled under bot profile.
botcfgratelimitprofile	<Double>	Read-only	Ratelimit enabled under bot profile.
botcfgsignatureprofile	<Double>	Read-only	Static Signatures enabled under bot profile.
botcfgdfpprofile	<Double>	Read-only	Device Fingerprint enabled under bot profile.
botcfgtpsprofile	<Double>	Read-only	TPS enabled under bot profile.
botcfgtrapprofile	<Double>	Read-only	Bot Trap enabled under bot profile.
botcfgkmdetectionprofile	<Double>	Read-only	Keyboard mouse detection enabled under bot profile.

Operations

(click to see Properties)

- GET (ALL)
- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/botprofile **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/botprofile? **args=name: <String_value> ,detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get botprofile resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/botprofile? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "botprofile": [ {

"name":<String_value>,

"botviolwhitelistlogprofile":<Double_value>,

"botvioltrapresetprofile":<Double_value>,

"bottotalresetprofile":<Double_value>,

"botviolcaptchaprofile":<Double_value>,

"botviolstaticsignaturelogprofilerate":<Double_value>,

"botredirectprofilerate":<Double_value>,

"botrequestsperprofile":<Double_value>,

"botcfgiprepprofile":<Double_value>,

"botviolipreputationcaptchaprofilerate":<Double_value>,

"botviolwhitelistlogprofilerate":<Double_value>,

"botvioltpslogprofilerate":<Double_value>,

"bottotaldropprofile":<Double_value>,

"botviolstaticsignatureredirectprofile":<Double_value>,

"botviolipreputationdropprofile":<Double_value>,

"botvioltpsprofile":<Double_value>,

"botviolipreputationprofile":<Double_value>,

"botcfgdfpprofile":<Double_value>,

"botrequestsperprofilerate":<Double_value>,
```

```
"botviolblacklistredirectprofilerate":<Double_value>,

"botvioldevicefingerprintresetprofilerate":<Double_value>,

"botviolratelimitexceededresponseprofilerate":<Double_value>,

"botviolblacklistresetprofile":<Double_value>,

"botviolcaptcharesetprofile":<Double_value>,

"botvioltpslogprofile":<Double_value>,

"botviolblacklistlogprofilerate":<Double_value>,

"botviolcaptchadropprofile":<Double_value>,

"botviolblacklistprofile":<Double_value>,

"botvioltpsdropprofile":<Double_value>,

"bottotallogprofile":<Double_value>,

"botvioltrapdropprofilerate":<Double_value>,

"botvioldevicefingerprintredirectprofile":<Double_value>,

"botviolstaticsignaturedropprofilerate":<Double_value>,

"botvioltpsredirectprofile":<Double_value>,

"botdropprofilerate":<Double_value>,

"botresbytesperprofile":<Double_value>,

"botvioltpscaptchaprofile":<Double_value>,

"botvioldevicefingerprintlogprofilerate":<Double_value>,

"botviolwhitelistprofile":<Double_value>,

"botvioliprepputationcaptchaprofile":<Double_value>,

"botcfgblacklistprofile":<Double_value>,
```

```
"botvioltpsprofilerate":<Double_value>,

"botviolratelimitredirectprofile":<Double_value>,

"botcfgtpsprofile":<Double_value>,

"botviolipreputationdropprofilerate":<Double_value>,

"botvioldevicefingerprintprofilerate":<Double_value>,

"botvioldevicefingerprintresetprofile":<Double_value>,

"botviolcaptcharedirectprofile":<Double_value>,

"botresetprofilerate":<Double_value>,

"botcfgkmdetectionprofile":<Double_value>,

"botviolcaptchalogprofile":<Double_value>,

"botvioldevicefingerprintcaptchaprofilerate":<Double_value>,

"botviolblacklistdropprofile":<Double_value>,

"botviolratelimitprofile":<Double_value>,

"botcfgsignatureprofile":<Double_value>,

"botresbytesperprofilerate":<Double_value>,

"botviolratelimitlogprofilerate":<Double_value>,

"botvioltrapprofilerate":<Double_value>,

"botcfgtrapprofile":<Double_value>,

"botviolratelimitresetprofilerate":<Double_value>,

"botvioldevicefingerprintdropprofilerate":<Double_value>,

"botviolblacklistredirectprofile":<Double_value>,

"botviolstaticsignatureredirectprofilerate":<Double_value>,
```

```
"botvioldevicefingerprintlogprofile":<Double_value>,

"botviolcaptchadropprofilerate":<Double_value>,

"botvioldevicefingerprintprofile":<Double_value>,

"botlogprofilerate":<Double_value>,

"botviolratelimitprofilerate":<Double_value>,

"botviolstaticsignatureresetprofile":<Double_value>,

"botreqbytesperprofilerate":<Double_value>,

"botviolstaticsignatureprofile":<Double_value>,

"botvioltrapdropprofile":<Double_value>,

"botvioldevicefingerprintdropprofile":<Double_value>,

"botviolstaticsignatureresetprofilerate":<Double_value>,

"botviolwhitelistprofilerate":<Double_value>,

"botvioliprepputationredirectprofile":<Double_value>,

"botviolstaticsignaturedropprofile":<Double_value>,

"botviolratelimitlogprofile":<Double_value>,

"botviolcaptchaprofilerate":<Double_value>,

"botvioltrapresetprofilerate":<Double_value>,

"botviolblacklistlogprofile":<Double_value>,

"botviolratelimitexceededresponseprofile":<Double_value>,

"botvioltpsredirectprofilerate":<Double_value>,

"botvioliprepputationlogprofile":<Double_value>,

"botviolratelimitdropprofile":<Double_value>,
```

```
"botcfgratelimitprofile":<Double_value>,

"botreqbytesperprofile":<Double_value>,

"botviolipreputationresetprofile":<Double_value>,

"botvioltrapredirectprofilerate":<Double_value>,

"botviolblacklistdropprofilerate":<Double_value>,

"botresponsesperprofile":<Double_value>,

"botvioltpscaptchaprofilerate":<Double_value>,

"botviolratelimitresetprofile":<Double_value>,

"botviolcaptcharesetprofilerate":<Double_value>,

"botvioldevicefingerprintcaptchaprofile":<Double_value>,

"botviolblacklistresetprofilerate":<Double_value>,

"botviolcaptchalogprofilerate":<Double_value>,

"botvioliprepputationlogprofilerate":<Double_value>,

"botviolratelimitredirectprofilerate":<Double_value>,

"botvioltrapredirectprofile":<Double_value>,

"botvioltpsdropprofilerate":<Double_value>,

"botvioltraplogprofilerate":<Double_value>,

"bottotalredirectprofile":<Double_value>,

"botcfgwhitelistprofile":<Double_value>,

"botvioliprepputationredirectprofilerate":<Double_value>,

"botviolblacklistprofilerate":<Double_value>,

"botviolstaticsignaturelogprofile":<Double_value>,
```

```
"botviolipreputationresetprofilerate":<Double_value>,

"botvioltraplogprofile":<Double_value>,

"botvioltrapprofile":<Double_value>,

"botvioltpsresetprofile":<Double_value>,

"botviolratelimitdropprofilerate":<Double_value>,

"botresponsesperprofilerate":<Double_value>,

"botvioltpsresetprofilerate":<Double_value>,

"botviolstaticsignatureprofilerate":<Double_value>,

"botvioliprepotationprofilerate":<Double_value>,

"botviolcaptcharedirectprofilerate":<Double_value>,

"botvioldevicefingerprintredirectprofilerate":<Double_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/stat/botprofile/ name_value><String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "botprofile": [ {

"name":<String_value>,

"botviolwhitelistlogprofile":<Double_value>,

"botvioltrapresetprofile":<Double_value>,

"bottotalresetprofile":<Double_value>,

"botviolcaptchaprofile":<Double_value>,

"botviolstaticsignaturelogprofilerate":<Double_value>,

"botredirectprofilerate":<Double_value>,

"botrequestsperprofile":<Double_value>,

"botcfgiprepprofile":<Double_value>,

"botviolipreputationcaptchaprofilerate":<Double_value>,

"botviolwhitelistlogprofilerate":<Double_value>,

"botvioltpslogprofilerate":<Double_value>,

"bottotaldropprofile":<Double_value>,

"botviolstaticsignatureredirectprofile":<Double_value>,

"botviolipreputationdropprofile":<Double_value>,

"botvioltpsprofile":<Double_value>,

"botviolipreputationprofile":<Double_value>,

"botcfgdfpprofile":<Double_value>,

"botrequestsperprofilerate":<Double_value>,

"botviolblacklistredirectprofilerate":<Double_value>,
```

```
"botvioldevicefingerprintresetprofilerate":<Double_value>,

"botviolratelimitexceededresponseprofilerate":<Double_value>,

"botviolblacklistresetprofile":<Double_value>,

"botviolcaptcharesetprofile":<Double_value>,

"botvioltpslogprofile":<Double_value>,

"botviolblacklistlogprofilerate":<Double_value>,

"botviolcaptchadropprofile":<Double_value>,

"botviolblacklistprofile":<Double_value>,

"botvioltpsdropprofile":<Double_value>,

"bottotallogprofile":<Double_value>,

"botvioltrapdropprofilerate":<Double_value>,

"botvioldevicefingerprintredirectprofile":<Double_value>,

"botviolstaticsignaturedropprofilerate":<Double_value>,

"botvioltpsredirectprofile":<Double_value>,

"botdropprofilerate":<Double_value>,

"botresbytesperprofile":<Double_value>,

"botvioltpscaptchaprofile":<Double_value>,

"botvioldevicefingerprintlogprofilerate":<Double_value>,

"botviolwhitelistprofile":<Double_value>,

"botvioliprepputationcaptchaprofile":<Double_value>,

"botcfgblacklistprofile":<Double_value>,

"botvioltpsprofilerate":<Double_value>,
```

```
"botviolratelimitredirectprofile":<Double_value>,

"botcfgtpsprofile":<Double_value>,

"botviolipreputationdropprofilerate":<Double_value>,

"botvioldevicefingerprintprofilerate":<Double_value>,

"botvioldevicefingerprintresetprofile":<Double_value>,

"botviolcaptcharedirectprofile":<Double_value>,

"botresetprofilerate":<Double_value>,

"botcfgkmdetectionprofile":<Double_value>,

"botviolcaptchalogprofile":<Double_value>,

"botvioldevicefingerprintcaptchaprofilerate":<Double_value>,

"botviolblacklistdropprofile":<Double_value>,

"botviolratelimitprofile":<Double_value>,

"botcfgsignatureprofile":<Double_value>,

"botresbytesperprofilerate":<Double_value>,

"botviolratelimitlogprofilerate":<Double_value>,

"botvioltrapprofilerate":<Double_value>,

"botcfgtrapprofile":<Double_value>,

"botviolratelimitresetprofilerate":<Double_value>,

"botvioldevicefingerprintdropprofilerate":<Double_value>,

"botviolblacklistredirectprofile":<Double_value>,

"botviolstaticsignatureredirectprofilerate":<Double_value>,

"botvioldevicefingerprintlogprofile":<Double_value>,
```

```
"botviolcaptchadropprofilerate":<Double_value>,

"botvioldevicefingerprintprofile":<Double_value>,

"botlogprofilerate":<Double_value>,

"botviolratelimitprofilerate":<Double_value>,

"botviolstaticsignatureresetprofile":<Double_value>,

"botreqbytesperprofilerate":<Double_value>,

"botviolstaticsignatureprofile":<Double_value>,

"botvioltrapdropprofile":<Double_value>,

"botvioldevicefingerprintdropprofile":<Double_value>,

"botviolstaticsignatureresetprofilerate":<Double_value>,

"botviolwhitelistprofilerate":<Double_value>,

"botvioliprepputationredirectprofile":<Double_value>,

"botviolstaticsignaturedropprofile":<Double_value>,

"botviolratelimitlogprofile":<Double_value>,

"botviolcaptchaprofilerate":<Double_value>,

"botvioltrapresetprofilerate":<Double_value>,

"botviolblacklistlogprofile":<Double_value>,

"botviolratelimitexceededresponseprofile":<Double_value>,

"botvioltpsredirectprofilerate":<Double_value>,

"botvioliprepputationlogprofile":<Double_value>,

"botviolratelimitdropprofile":<Double_value>,

"botcfgratelimitprofile":<Double_value>,
```

```
"botreqbytesperprofile":<Double_value>,

"botviolipreputationresetprofile":<Double_value>,

"botvioltrapredirectprofilerate":<Double_value>,

"botviolblacklistdropprofilerate":<Double_value>,

"botresponsesperprofile":<Double_value>,

"botvioltpscaptchaprofilerate":<Double_value>,

"botviolratelimitresetprofile":<Double_value>,

"botviolcaptcharesetprofilerate":<Double_value>,

"botvioldevicefingerprintcaptchaprofile":<Double_value>,

"botviolblacklistresetprofilerate":<Double_value>,

"botviolcaptchalogprofilerate":<Double_value>,

"botvioliprepputationlogprofilerate":<Double_value>,

"botviolratelimitredirectprofilerate":<Double_value>,

"botvioltrapredirectprofile":<Double_value>,

"botvioltpsdropprofilerate":<Double_value>,

"botvioltraplogprofilerate":<Double_value>,

"bottotalredirectprofile":<Double_value>,

"botcfgwhitelistprofile":<Double_value>,

"botvioliprepputationredirectprofilerate":<Double_value>,

"botviolblacklistprofilerate":<Double_value>,

"botviolstaticsignaturelogprofile":<Double_value>,

"botvioliprepputationresetprofilerate":<Double_value>,
```

```
"botvioltraplogprofile":<Double_value>,

"botvioltrapprofile":<Double_value>,

"botvioltpsresetprofile":<Double_value>,

"botviolratelimitdropprofilerate":<Double_value>,

"botresponsesperprofilerate":<Double_value>,

"botvioltpsresetprofilerate":<Double_value>,

"botviolstaticsignatureprofilerate":<Double_value>,

"botvioliprepputationprofilerate":<Double_value>,

"botviolcaptcharedirectprofilerate":<Double_value>,

"botvioldevicefingerprintredirectprofilerate":<Double_value>

}]}
```

cache

Integrated Caching

Integrated Caching statistics. The Integrated Caching feature is used to cache static and dynamic web application data.

NAME	DESCRIPTION
cache	Statistics for cache.
cachecontentgroup	Statistics for Integrated Cache content group resource.
cachepolicy	Statistics for Integrated Cache policy resource.

NAME	DESCRIPTION
cachepolicylabel	Statistics for cache policy label resource.

cache

Statistics for cache.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full
cachemaxmemorykb	<Double>	Read-only	Largest amount of memory the Citrix ADC can dedicate to caching, up to 50% of available memory. A 0 value disables caching, but the caching module continues to run.
cacherecentpercentsuccessfulrevalidation	<Double>	Read-only	Recently recorded percentage of times stored content was successfully revalidated by a 304 response rather than by a full response
cacherecentpercentstoreablemiss	<Double>	Read-only	Recently recorded ratio of store-able misses to all misses expressed as percentage.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
cacherecentpercentparameterizedhits	<Double>	Read-only	Recently recorded ratio of parameterized 304 hits to all parameterized hits expressed as a percentage
cacherecentpercentoriginbandwidthsaved	<Double>	Read-only	Bytes served from cache divided by total bytes served to client. This ratio can be greater than 1 because of the assumption that all compression has been done in the Citrix ADC.
cacherecentpercenthit	<Double>	Read-only	Recently recorded cache hit ratio expressed as percentage
cacherecentpercentbytehit	<Double>	Read-only	Recently recorded cache byte hit ratio expressed as percentage. Here we define byte hit ratio as ((number of bytes served from the cache)/(total number of bytes served to the client)). This is the standard definition of Byte Hit Ratio. If compression is turned ON in NS then this ratio doesn't mean much. This might under or

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			over estimate the origin-to-cache bandwidth saving (depending upon whether bytes served by CMP in Citrix ADC are more or less than compressed bytes served from the cache). If CMP is turned OFF in NS then this ratio is same as cacheRecentPercentOriginBandwidthSaved.
cacherecentpercent304hits	<Double>	Read-only	Recently recorded ratio of 304 hits to all hits expressed as percentage
cacheutilizedmemorykb	<Double>	Read-only	Amount of memory the integrated cache is currently using.
cachemaxmemoryactivekb	<Double>	Read-only	Currently active value of maximum memory
cache64maxmemorykb	<Double>	Read-only	Largest amount of memory the Citrix ADC can dedicate to caching, up to 50% of available memory. A 0 value disables caching, but the caching module continues to run.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
cachepercentpethits	<Double>	Read-only	Percentage of cache hits in content groups that have Poll Every Time enabled, relative to all searches of content groups with Poll Every Time enabled.
cachetotpethits	<Double>	Read-only	Number of times a cache hit was found during a search of a content group that has Poll Every Time enabled.
cachepethitsrate	<Double>	Read-only	Rate (/s) counter for cachetotpethits
cachepercentparameterized304hits	<Double>	Read-only	Percentage of parameterized 304 hits relative to all parameterized hits.
cachetotparameterizedhits	<Double>	Read-only	Parameterized requests resulting in either a 304 or non-304 hit.
cacheparameterizedhitsrate	<Double>	Read-only	Rate (/s) counter for cachetotparameterizedhits
cachepercentsuccessfulrevalidation	<Double>	Read-only	Percentage of times stored content was successfully revalidated by a 304 (Object Not Modifed) response rather than by a full response

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
cachepercentstoreablemiss	<Double>	Read-only	Responses that were fetched from the origin, stored in the cache, and then served to the client, as a percentage of all cache misses.
cachetotfulltoconditionalrequest	<Double>	Read-only	Number of user-agent requests for a cached Poll Every Time (PET) response that were sent to the origin server as conditional requests.
cachefulltoconditionalrequestrate	<Double>	Read-only	Rate (/s) counter for cachetotfulltoconditionalrequest
cachetotsuccessfulrevalidation	<Double>	Read-only	Total number of times stored content was successfully revalidated by a 304 Not Modified response from the origin.
cachesuccessfulrevalidationrate	<Double>	Read-only	Rate (/s) counter for cachetotsuccessfulrevalidation
cachetotrevalidationmiss	<Double>	Read-only	Responses that an intervening cache revalidated with the integrated cache before serving, as determined by a Cache-Control: Max-Age header

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			configurable in the integrated cache
cacherevalidationmissrate	<Double>	Read-only	Rate (/s) counter for cachetotrevalidation miss
cachetotnonstoreablemisses	<Double>	Read-only	Cache misses for which the fetched response is not stored in the cache. These responses match policies with a NOCACHE action or are affected by Poll Every Time.
cachenonstoreablemissesrate	<Double>	Read-only	Rate (/s) counter for cachetotnonstoreablemisses
cachetotstoreablemisses	<Double>	Read-only	Cache misses for which the fetched response is stored in the cache before serving it to the client. Storable misses conform to a built-in or user-defined caching policy that contains a CACHE action.
cachestoreablemissesrate	<Double>	Read-only	Rate (/s) counter for cachetotstoreablemisses
cachecompressedbytesserved	<Double>	Read-only	Number of compressed bytes served from the cache

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
cachecompressedbytesservedrate	<Double>	Read-only	Rate (/s) counter for cachecompressedbytesserved
cachepercentbytehit	<Double>	Read-only	Bytes served from the cache divided by total bytes served to the client. If compression is On in the Citrix ADC, this ratio may not reflect the bytes served by the compression module. If the compression is Off, this ratio is the same as cachePercentOriginBandwidthSaved.
cachebytesserved	<Double>	Read-only	Total number of bytes served from the integrated cache
cachebytesservedrate	<Double>	Read-only	Rate (/s) counter for cachebytesserved
cachetotresponsebytes	<Double>	Read-only	Total number of HTTP response bytes served by Citrix ADC from both the origin and the cache
cacheresponsebytesrate	<Double>	Read-only	Rate (/s) counter for cachetotresponsebytes
cachepercent304hits	<Double>	Read-only	304 responses as a percentage of all

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			responses that the Citrix ADC served.
cachenummarker	<Double>	Read-only	Marker objects created when a response exceeds the maximum or minimum size for entries in its content group or has not yet received the minimum number of hits required for items in its content group.
cachepercentoriginbandwidthsaved	<Double>	Read-only	Percentage of origin bandwidth saved, expressed as number of bytes served from the integrated cache divided by all bytes served. The assumption is that all compression is done in the Citrix ADC.
cachepercenthit	<Double>	Read-only	Cache hits as percentage of the total number of requests
cachetotmisses	<Double>	Read-only	Intercepted HTTP requests requiring fetches from origin server.
cachemissesrate	<Double>	Read-only	Rate (/s) counter for cachetotmisses

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
cachetothits	<Double>	Read-only	Responses served from the integrated cache. These responses match a policy with a CACHE action.
cachehitsrate	<Double>	Read-only	Rate (/s) counter for cachetothits
cachetotrequests	<Double>	Read-only	Total cache hits plus total cache misses.
cacherequestsrate	<Double>	Read-only	Rate (/s) counter for cachetotrequests
cachenumcached	<Double>	Read-only	Responses currently in integrated cache. Includes responses fully downloaded, in the process of being downloaded, and expired or flushed but not yet removed.
cachecurhits	<Double>	Read-only	This number should be close to the number of hits being served currently.
cachecurmisses	<Double>	Read-only	Responses fetched from the origin and served from the cache. Should approximate storable misses. Does not include non-storable misses.
cachetotnon304hits	<Double>	Read-only	Total number of full (non-304) responses

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			served from the cache. A 304 status code indicates that a response has not been modified since the last time it was served
cachenon304hitsrate	<Double>	Read-only	Rate (/s) counter for cachetotnon304hits
cachetot304hits	<Double>	Read-only	Object not modified responses served from the cache. (Status code 304 served instead of the full response.)
cache304hitsrate	<Double>	Read-only	Rate (/s) counter for cachetot304hits
cachetotsqlhits	<Double>	Read-only	sql response served from cache
cachesqlhitsrate	<Double>	Read-only	Rate (/s) counter for cachetotsqlhits
cachetotexpireatlastbyte	<Double>	Read-only	Instances of content expiring immediately after receiving the last body byte due to the Expire at Last Byte setting for the content group.
cacheexpireatlastbyterate	<Double>	Read-only	Rate (/s) counter for cachetotexpireatlastbyte
cachetotflashcachemisses	<Double>	Read-only	Number of requests to a content group with flash cache

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			enabled that were cache misses. Flash cache distributes the response to all the clients in aqueue.
cacheflashcachemissesrate	<Double>	Read-only	Rate (/s) counter for cachetotflashcachemisses
cachetotflashcachehits	<Double>	Read-only	Number of requests to a content group with flash cache enabled that were cache hits. The flash cache setting queues requests that arrive simultaneously and distributes the response to all the clients in the queue.
cacheflashcachehitsrate	<Double>	Read-only	Rate (/s) counter for cachetotflashcachehits
cachetotparameterizedinvalidationrequests	<Double>	Read-only	Requests matching a policy with an invalidation (INVAL) action and a content group that uses an invalidation selector or parameters.
cacheparameterizedinvalidationrequestsrate	<Double>	Read-only	Rate (/s) counter for cachetotparameterizedinvalidationrequests

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
cachetotnonparameterizedinvalidationrequests	<Double>	Read-only	Requests that match an invalidation policy where the invalGroups parameter is configured and expires one or more content groups.
cachenonparameterizedinvalidationrequestsrate	<Double>	Read-only	Rate (/s) counter for cachetotnonparameterizedinvalidationrequests
cachetotinvalidationrequests	<Double>	Read-only	Requests that match an invalidation policy and result in expiration of specific cached responses or entire content groups.
cacheinvalidationrequestsrate	<Double>	Read-only	Rate (/s) counter for cachetotinvalidationrequests
cachetotparameterizedrequests	<Double>	Read-only	Total number of requests where the content group has hit and invalidation parameters or selectors.
cacheparameterizedrequestsrate	<Double>	Read-only	Rate (/s) counter for cachetotparameterizedrequests
cachetotparameterizednon304hits	<Double>	Read-only	Parameterized requests resulting in a full response (not status code 304:

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Object Not Updated) served from the cache.
cacheparameterized non304hitsrate	<Double>	Read-only	Rate (/s) counter for cachetotparameterized non304hits
cachetotparameterized304hits	<Double>	Read-only	Parameterized requests resulting in an object not modified (status code 304) response.
cacheparameterized 304hitsrate	<Double>	Read-only	Rate (/s) counter for cachetotparameterized304hits
cachetotpetrequests	<Double>	Read-only	Requests that triggered a search of a content group that has Poll Every Time (PET) enabled (always consult the origin server before serving cached data).
cachepetrequestsrate	<Double>	Read-only	Rate (/s) counter for cachetotpetrequests
cacheerrmemalloc	<Double>	Read-only	Total number of times the cache failed to allocate memory to store responses.
cachelargestresponsereceived	<Double>	Read-only	Size, in bytes, of largest response sent to client from

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			the cache or the origin server.

Operations

(click to see Properties)

- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/cache **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/cache? **args=detail: <Boolean_value> ,fullvalues:**

<Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>

Use this query-parameter to get cache resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/cache? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "cache": [ {

"cachetotsuccessfulrevalidation":<Double_value>,

"cachetotparameterized304hits":<Double_value>,

"cachepercentstoreablemiss":<Double_value>,

"cacheparameterizedrequestsrate":<Double_value>,

"cachepercentoriginbandwidthsaved":<Double_value>,

"cachetotmisses":<Double_value>,

"cachetothits":<Double_value>,

"cacherecentpercentparameterizedhits":<Double_value>,
```

```
"cachetotnonparameterizedinvalidationrequests":<Double_value>,

"cacheparameterizedinvalidationrequestsrate":<Double_value>,

"cacherevalidationmissrate":<Double_value>,

"cachemaxmemorykb":<Double_value>,

"cachenonstoreablemissesrate":<Double_value>,

"cachenumcached":<Double_value>,

"cacheresponsebytesrate":<Double_value>,

"cacherecentpercentstoreablemiss":<Double_value>,

"cachetotnonstoreablemisses":<Double_value>,

"cachetotpethits":<Double_value>,

"cachepethitsrate":<Double_value>,

"cachepercentsuccessfulrevalidation":<Double_value>,

"cacheexpireatlastbyterate":<Double_value>,

"cachenonparameterizedinvalidationrequestsrate":<Double_value>,

"cacheutilizedmemorykb":<Double_value>,

"cacherecentpercentbytehit":<Double_value>,

"cachetotsqlhits":<Double_value>,

"cachesuccessfulrevalidationrate":<Double_value>,

"cachetotparameterizedhits":<Double_value>,

"cachecompressedbytesservedrate":<Double_value>,

"cachepercentbytehit":<Double_value>,

"cacherecentpercent304hits":<Double_value>,
```

```
"cacherecentpercentoriginbandwidthsaved":<Double_value>,

"cache304hitsrate":<Double_value>,

"cachetot304hits":<Double_value>,

"cacheflashcachehitsrate":<Double_value>,

"cachetotparameterizednon304hits":<Double_value>,

"cachepercenthit":<Double_value>,

"cachetotstoreablemisses":<Double_value>,

"cachetotfulltoconditionalrequest":<Double_value>,

"cacheparameterized304hitsrate":<Double_value>,

"cachetotflashcachehits":<Double_value>,

"cacherequestsrate":<Double_value>,

"cachecurmisses":<Double_value>,

"cachecurhits":<Double_value>,

"cachenummarker":<Double_value>,

"cachemissesrate":<Double_value>,

"cachetotexpireatlastbyte":<Double_value>,

"cacherecentpercenthit":<Double_value>,

"cacheflashcachemissesrate":<Double_value>,

"cacheparameterizednon304hitsrate":<Double_value>,

"cachetotparameterizedinvalidationrequests":<Double_value>,

"cachetotrequests":<Double_value>,

"cachecompressedbytesserved":<Double_value>,
```

```
"cachetotpetrequests":<Double_value>,

"cachefulltoconditionalrequestrate":<Double_value>,

"cachepercentparameterized304hits":<Double_value>,

"cachemaxmemoryactivekb":<Double_value>,

"cachebytesservedrate":<Double_value>,

"cachebytesserved":<Double_value>,

"cachepercent304hits":<Double_value>,

"cachelargestresponsereceived":<Double_value>,

"cachehitsrate":<Double_value>,

"cachestoreablemissesrate":<Double_value>,

"cachetotflashcachemisses":<Double_value>,

"cachetotnon304hits":<Double_value>,

"cachepetrequestsrate":<Double_value>,

"cachetotresponsebytes":<Double_value>,

"cacheparameterizedhitsrate":<Double_value>,

"cachesqlhitsrate":<Double_value>,

"cachetotrevalidationmiss":<Double_value>,

"cachetotparameterizedrequests":<Double_value>,

"cache64maxmemorykb":<Double_value>,

"cachetotinvalidationrequests":<Double_value>,

"cachenon304hitsrate":<Double_value>,

"cacherecentpercentsuccessfulrevalidation":<Double_value>,
```

```
"cacheinvalidationrequestsrate":<Double_value>,

"cachepercentpethits":<Double_value>,

"cacheerrmemalloc":<Double_value>

}]}
```

cachecontentgroup

Statistics for Integrated Cache content group resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the cache contentgroup for which to display statistics. If you do not set this parameter, statistics are shown for all cache contentgroups. Minimum length = 1
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full
groupnon304hit	<Double>	Read-only	Non304 hits for ContentGroup
group304hit	<Double>	Read-only	304 hits for ContentGroup

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
totcell	<Double>	Read-only	Number of objects in contentgroup
totmarkercell	<Double>	Read-only	Number of marker objects in contentgroup
timesflushed	<Double>	Read-only	Number of times contentgroup is flushed
totmemory	<Double>	Read-only	current memory usage
maxmemory	<Double>	Read-only	maximum memory usage limit

Operations

(click to see Properties)

- GET (ALL)
- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/cachecontentgroup **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/cachecontentgroup? **args=name: <String_value> ,detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get cachecontentgroup resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/cachecontentgroup? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "cachecontentgroup": [ {

"name":<String_value>,
```

```
"totcell":<Double_value>,

"group304hit":<Double_value>,

"totmemory":<Double_value>,

"maxmemory":<Double_value>,

"groupnon304hit":<Double_value>,

"timesflushed":<Double_value>,

"totmarkercell":<Double_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/stat/cachecontentgroup/ name_value><String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "cachecontentgroup": [ {

"name":<String_value>,

"totcell":<Double_value>,
```

```
"group304hit":<Double_value>,

"totmemory":<Double_value>,

"maxmemory":<Double_value>,

"groupnon304hit":<Double_value>,

"timesflushed":<Double_value>,

"totmarkercell":<Double_value>

}]}
```

cachepolicy

Statistics for Integrated Cache policy resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
policyname	<String>	Read-write	Name of the cache policy for which to display statistics. If you do not set this parameter, statistics are shown for all cache policies. Minimum length = 1
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full
pipolicyhits	<Double>	Read-only	Number of hits on the policy

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
pipolicyhitsrate	<Double>	Read-only	Rate (/s) counter for pipolicyhits
pipolicyundefhits	<Double>	Read-only	Number of undef hits on the policy
pipolicyundefhitsrate	<Double>	Read-only	Rate (/s) counter for pipolicyundefhits

Operations

(click to see Properties)

- GET (ALL)
- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.
- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/cachepolicy **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/cachepolicy? **args=policyname: <String_value> ,detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get cachepolicy resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/cachepolicy? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "cachepolicy": [ {

"policyname":<String_value>,

"pipolicyhitsrate":<Double_value>,

"pipolicyundefhitsrate":<Double_value>,

"pipolicyhits":<Double_value>,
```

```
"pipolicyundefhits":<Double_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/stat/cachepolicy/ policyname_value><String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "cachepolicy": [ {

"policyname":<String_value>,

"pipolicyhitsrate":<Double_value>,

"pipolicyundefhitsrate":<Double_value>,

"pipolicyhits":<Double_value>,

"pipolicyundefhits":<Double_value>

}]}
```

cachepolicylabel

Statistics for cache policy label resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
labelname	<String>	Read-write	Name of the cache-policy label for which to display statistics. If you do not set this parameter statistics are shown for all cache-policy labels. Minimum length = 1
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full
pipolicylabelhits	<Double>	Read-only	Number of times policy label was invoked.
pipolicylabelhitsrate	<Double>	Read-only	Rate (/s) counter for pipolicylabelhits

Operations

(click to see Properties)

- GET (ALL)
- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/cachepolicylabel **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/cachepolicylabel? **args=labelname: <String_value> ,detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get cachepolicylabel resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/cachepolicylabel? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "cachepolicylabel": [ {

"labelname":<String_value>,

"pipolicylabelhitsrate":<Double_value>,

"pipolicylabelhits":<Double_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/stat/cachepolicylabel/ labelname_value><String>
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "cachepolicylabel": [ {

"labelname":<String_value>,

"pipolicylabelhitsrate":<Double_value>,

"pipolicylabelhits":<Double_value>

}]}
```

cloud

Cloud

Citrix ADC as SD proxy statistics and cloud discovery commands.

NAME	DESCRIPTION
cloud	Statistics for cloud.

cloud

Statistics for cloud.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full
ngsshieldle1secclxmtpconnesttime	<Double>	Read-only	Total Connection with CLXMTP connect time less than 1 sec

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ngsshieldle1secclxmtpconnesttimerate	<Double>	Read-only	Rate (/s) counter for ngsshieldle1secclxmtpconnesttime
ngsshieldle2secclxmtpconnesttime	<Double>	Read-only	Total Connection with CLXMTP connect time less than 2 sec
ngsshieldle2secclxmtpconnesttimerate	<Double>	Read-only	Rate (/s) counter for ngsshieldle2secclxmtpconnesttime
ngsshieldle3secclxmtpconnesttime	<Double>	Read-only	Total Connection with CLXMTP connect time less than 3 sec
ngsshieldle3secclxmtpconnesttimerate	<Double>	Read-only	Rate (/s) counter for ngsshieldle3secclxmtpconnesttime
ngsshieldle5secclxmtpconnesttime	<Double>	Read-only	Total Connection with CLXMTP connect time less than 5 sec
ngsshieldle5secclxmtpconnesttimerate	<Double>	Read-only	Rate (/s) counter for ngsshieldle5secclxmtpconnesttime
ngsshieldle8secclxmtpconnesttime	<Double>	Read-only	Total Connection with CLXMPT connect time less than 8 sec
ngsshieldle8secclxmtpconnesttimerate	<Double>	Read-only	Rate (/s) counter for ngsshieldle8secclxmtpconnesttime

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ngsshieldle13secclx mtpconnesttime	<Double>	Read-only	Total Connection with CLXMPT connect time less than 13 sec
ngsshieldle13secclx mtpconnesttimerate	<Double>	Read-only	Rate (/s) counter for ngsshieldle13secclx mtpconnesttime
ngsshieldle21secclx mtpconnesttime	<Double>	Read-only	Total Connection with CLXMPT connect time less than 21 sec
ngsshieldle21secclx mtpconnesttimerate	<Double>	Read-only	Rate (/s) counter for ngsshieldle21secclx mtpconnesttime
ngsshieldgt21secclx mtpconnesttime	<Double>	Read-only	Total Connection with CLXMPT connect time greater than 21 sec
ngsshieldgt21secclx mtpconnesttimerate	<Double>	Read-only	Rate (/s) counter for ngsshieldgt21secclx mtpconnesttime
ngsgctle1secconnest time	<Double>	Read-only	Total Connection with GCT connect time less than 1 sec
ngsgctle1secconnest timerate	<Double>	Read-only	Rate (/s) counter for ngsgctle1secconnest time
ngsgctle2secconnest time	<Double>	Read-only	Total Connection with GCT connect time less than 2 sec

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ngsgctle2secconnesttimerate	<Double>	Read-only	Rate (/s) counter for ngsgctle2secconnesttime
ngsgctle3secconnesttime	<Double>	Read-only	Total Connection with GCT connect time less than 3 sec
ngsgctle3secconnesttimerate	<Double>	Read-only	Rate (/s) counter for ngsgctle3secconnesttime
ngsgctle5secconnesttime	<Double>	Read-only	Total Connection with GCT connect time less than 5 sec
ngsgctle5secconnesttimerate	<Double>	Read-only	Rate (/s) counter for ngsgctle5secconnesttime
ngsgctle8secconnesttime	<Double>	Read-only	Total Connection with GCT connect time less than 8 sec
ngsgctle8secconnesttimerate	<Double>	Read-only	Rate (/s) counter for ngsgctle8secconnesttime
ngsgctgt8secconnesttime	<Double>	Read-only	Total Connection with GCT connect time greater than 8 sec
ngsgctgt8secconnesttimerate	<Double>	Read-only	Rate (/s) counter for ngsgctgt8secconnesttime
ngsshieldclxmtpconnestattempted	<Double>	Read-only	Total attempted CLXMTP connection

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ngsshieldclxmtpconnestattemptedrate	<Double>	Read-only	Rate (/s) counter for ngsshieldclxmtpconnestattempted
ngsshieldclxmtpconnestsuccess	<Double>	Read-only	Total successful CLXMTP connection
ngsshieldclxmtpconnestsuccessrate	<Double>	Read-only	Rate (/s) counter for ngsshieldclxmtpconnestsuccess
ngsshieldclxmtpsoftdeny	<Double>	Read-only	Total number of softdeny received by SN
ngsshieldclxmtpsoftdenyrate	<Double>	Read-only	Rate (/s) counter for ngsshieldclxmtpsoftdeny
ngsshieldclxmtpdeny	<Double>	Read-only	Total number of deny received by SN
ngsshieldclxmtpdenyrate	<Double>	Read-only	Rate (/s) counter for ngsshieldclxmtpdeny
ngsshieldclxmtpallowtarget	<Double>	Read-only	Total number of allowtarget received by SN
ngsshieldclxmtpallowtargetrate	<Double>	Read-only	Rate (/s) counter for ngsshieldclxmtpallowtarget
ngsshieldclxmtpredirecttarget	<Double>	Read-only	Total number of redirecttarget received by SN
ngsshieldclxmtpredirecttargetrate	<Double>	Read-only	Rate (/s) counter for ngsshieldclxmtpredirecttarget

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ngsshieldclxmtpconnectorfanouttimeout	<Double>	Read-only	Total number of fanout timeout
ngsshieldclxmtpconnectorfanouttimeoutrate	<Double>	Read-only	Rate (/s) counter for ngsshieldclxmtpconnectorfanouttimeout
ngsshieldclxmtpglobalfanouttimeout	<Double>	Read-only	Total number of global fanout timeout
ngsshieldclxmtpglobalfanouttimeoutrate	<Double>	Read-only	Rate (/s) counter for ngsshieldclxmtpglobalfanouttimeout
ngsshieldfanout	<Double>	Read-only	Total number of fanout
ngsshieldfanoutrate	<Double>	Read-only	Rate (/s) counter for ngsshieldfanout
ngsshieldclvalidationfailure	<Double>	Read-only	Total Connection lease validation failure
ngsshieldclvalidationfailurerate	<Double>	Read-only	Rate (/s) counter for ngsshieldclvalidationfailure
ngsshieldcldecryptionfailure	<Double>	Read-only	Total Connection lease decryption failure
ngsshieldcldecryptionfailurerate	<Double>	Read-only	Rate (/s) counter for ngsshieldcldecryptionfailure
ngsshieldclxmtpcomplete	<Double>	Read-only	Total CLXMTP completed

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ngsshieldclxmtpcompleterate	<Double>	Read-only	Rate (/s) counter for ngsshieldclxmtpcomplete
ngsshieldclxmtptrustestfailure	<Double>	Read-only	Total CLXMTP trust establishment failure
ngsshieldclxmtptrustestfailurerate	<Double>	Read-only	Rate (/s) counter for ngsshieldclxmtptrustestfailure
ngsshieldclxmtppubkeyvalfailure	<Double>	Read-only	Total CLXMTP pub key validation failure
ngsshieldclxmtppubkeyvalfailurerate	<Double>	Read-only	Rate (/s) counter for ngsshieldclxmtppubkeyvalfailure
ngsshieldclxmtpconnvalidationfailure	<Double>	Read-only	Total CLXMTP connection lease validation failure
ngsshieldclxmtpconnvalidationfailurerate	<Double>	Read-only	Rate (/s) counter for ngsshieldclxmtpconnvalidationfailure
ngsshieldclxmtpauthorizeconnreqfailure	<Double>	Read-only	Total CLXMTP authorize connection request failure
ngsshieldclxmtpauthorizeconnreqfailurerate	<Double>	Read-only	Rate (/s) counter for ngsshieldclxmtpauthorizeconnreqfailure
ngsshieldkeyfetchfailure	<Double>	Read-only	Total Shield key fetching failure
ngsshieldkeyfetchfailurerate	<Double>	Read-only	Rate (/s) counter for ngsshieldkeyfetchfailure

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ngsshielddemandedrtkeynotfound	<Double>	Read-only	Total root of trust keys not found failure
ngsshielddemandedrtkeynotfoundrate	<Double>	Read-only	Rate (/s) counter for ngsshielddemandedrtkeynotfound
ngsshielddemandedcliskeynotfound	<Double>	Read-only	Total CLIS keys not found failure
ngsshielddemandedcliskeynotfoundrate	<Double>	Read-only	Rate (/s) counter for ngsshielddemandedcliskeynotfound
ngsshielddemandedgwkeynotfound	<Double>	Read-only	Total gateway keys not found failure
ngsshielddemandedgwkeynotfoundrate	<Double>	Read-only	Rate (/s) counter for ngsshielddemandedgwkeynotfound
ngsshieldkeycacheempty	<Double>	Read-only	Total shield key cache list empty
ngsshieldkeycacheemptyrate	<Double>	Read-only	Rate (/s) counter for ngsshieldkeycacheempty
ngsshieldakvgetsecretlistfailure	<Double>	Read-only	Total failures to get akv secret list
ngsshieldakvgetsecretlistfailurerate	<Double>	Read-only	Rate (/s) counter for ngsshieldakvgetsecretlistfailure
ngsshieldakvgetsecretfailure	<Double>	Read-only	Total failures to get akv secrets

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ngsshieldakvgetsecretfailurerate	<Double>	Read-only	Rate (/s) counter for ngsshieldakvgetsecretfailure
ngsshieldakvtokenfailure	<Double>	Read-only	Total akv token failures
ngsshieldakvtokenfailurerate	<Double>	Read-only	Rate (/s) counter for ngsshieldakvtokenfailure
ngsshieldawssmgetmastersecretfailure	<Double>	Read-only	Total failures to get aws master secret list
ngsshieldawssmgetmastersecretfailurerate	<Double>	Read-only	Rate (/s) counter for ngsshieldawssmgetmastersecretfailure
ngsshieldawssmgetsecretfailure	<Double>	Read-only	Total failures to get aws secrets
ngsshieldawssmgetsecretfailurerate	<Double>	Read-only	Rate (/s) counter for ngsshieldawssmgetsecretfailure
ngsshieldawssmtokenfailure	<Double>	Read-only	Total aws secret manager token failures
ngsshieldawssmtokenfailurerate	<Double>	Read-only	Rate (/s) counter for ngsshieldawssmtokenfailure
ngsrendezvousv1launchsuccess	<Double>	Read-only	Total rendezvous v1 launch success
ngsrendezvousv1launchsuccessrate	<Double>	Read-only	Rate (/s) counter for ngsrendezvousv1launchsuccess

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ngsrendezvousv1launchfailure	<Double>	Read-only	Total rendezvous v1 launch failures
ngsrendezvousv1launchfailurerate	<Double>	Read-only	Rate (/s) counter for ngsrendezvousv1launchfailure
ngsrendezvousv2launchsuccess	<Double>	Read-only	Total rendezvous v2 launch success
ngsrendezvousv2launchsuccessrate	<Double>	Read-only	Rate (/s) counter for ngsrendezvousv2launchsuccess
ngsrendezvousv2launchfailure	<Double>	Read-only	Total rendezvous v2 launch failures
ngsrendezvousv2launchfailurerate	<Double>	Read-only	Rate (/s) counter for ngsrendezvousv2launchfailure
ngsrendezvousv1sntcntcmdfailure	<Double>	Read-only	Total rendezvous v1 sent connect command failure
ngsrendezvousv1sntcntcmdfailurerate	<Double>	Read-only	Rate (/s) counter for ngsrendezvousv1sntcntcmdfailure
ngsrendezvousv2sntcntcmdfailure	<Double>	Read-only	Total rendezvous v2 sent connect command failure
ngsrendezvousv2sntcntcmdfailurerate	<Double>	Read-only	Rate (/s) counter for ngsrendezvousv2sntcntcmdfailure
ngsrendezvousv2fallbacktov1	<Double>	Read-only	Total rendezvous v2 to v1 fallback

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ngsrendezvousv2fallbacktov1rate	<Double>	Read-only	Rate (/s) counter for ngsrendezvousv2fallbacktov1
ngsrendezvousv2delayedresponse	<Double>	Read-only	Total rendezvous v2 delayed response
ngsrendezvousv2delayedresponserate	<Double>	Read-only	Rate (/s) counter for ngsrendezvousv2delayedresponse
ngsrendezvousv2invalidcapability	<Double>	Read-only	Total invalid rendezvous capability received
ngsrendezvousv2invalidcapabilityrate	<Double>	Read-only	Rate (/s) counter for ngsrendezvousv2invalidcapability
ngsle1secconnesttime	<Double>	Read-only	Total connection with NGS connect less than 1 sec
ngsle1secconnesttimerate	<Double>	Read-only	Rate (/s) counter for ngsle1secconnesttime
ngsle2secconnesttime	<Double>	Read-only	Total connection with NGS connect less than 2 sec
ngsle2secconnesttimerate	<Double>	Read-only	Rate (/s) counter for ngsle2secconnesttime
ngsle3secconnesttime	<Double>	Read-only	Total connection with NGS connect less than 3 sec

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ngsle3secconnesttimerate	<Double>	Read-only	Rate (/s) counter for ngsle3secconnesttime
ngsle5secconnesttime	<Double>	Read-only	Total connection with NGS connect less than 5 sec
ngsle5secconnesttimerate	<Double>	Read-only	Rate (/s) counter for ngsle5secconnesttime
ngsle8secconnesttime	<Double>	Read-only	Total connection with NGS connect less than 8 sec
ngsle8secconnesttimerate	<Double>	Read-only	Rate (/s) counter for ngsle8secconnesttime
ngsgt8secconnesttime	<Double>	Read-only	Total connection with NGS connect greater than 8 sec
ngsgt8secconnesttimerate	<Double>	Read-only	Rate (/s) counter for ngsgt8secconnesttime
ngsapplaunchattempted	<Double>	Read-only	Total app launch attempted
ngsapplaunchattemptedrate	<Double>	Read-only	Rate (/s) counter for ngsapplaunchattempted
ngsapplaunchsuccess	<Double>	Read-only	Total app launch success
ngsapplaunchsuccessrate	<Double>	Read-only	Rate (/s) counter for ngsapplaunchsuccess

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ngsapplaunchfailure	<Double>	Read-only	Total app launch failures
ngsapplaunchfailurerate	<Double>	Read-only	Rate (/s) counter for ngsapplaunchfailure
ngsstavalfailure	<Double>	Read-only	Total STA validation failures
ngsstavalfailurerate	<Double>	Read-only	Rate (/s) counter for ngsstavalfailure
ngsstavalsuccess	<Double>	Read-only	Total STA validation success
ngsstavalsuccessrate	<Double>	Read-only	Rate (/s) counter for ngsstavalsuccess
ngsticketsvcdown	<Double>	Read-only	Total Ticket service down
ngsticketsvcdownrate	<Double>	Read-only	Rate (/s) counter for ngsticketsvcdown
ngsdelayedconnectorresponse	<Double>	Read-only	Total delayed response received from connector
ngsdelayedconnectorresponserate	<Double>	Read-only	Rate (/s) counter for ngsdelayedconnectorresponse
ngstunnelclosedbyclient	<Double>	Read-only	Total number of tunnels closed by client
ngstunnelclosedbyclientrate	<Double>	Read-only	Rate (/s) counter for ngstunnelclosedbyclient

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ngstunnelclosedbyvda	<Double>	Read-only	Total number of tunnels closed by VDA
ngstunnelclosedbyvdarate	<Double>	Read-only	Rate (/s) counter for ngstunnelclosedbyvda
ngsconncmdfailbyfr	<Double>	Read-only	Total number fo coonect command failed by FR
ngsconncmdfailbyfrrate	<Double>	Read-only	Rate (/s) counter for ngsconncmdfailbyfr
ngsconncmdfailclientconnnotfound	<Double>	Read-only	Totla connect command failed with client connection not found
ngsconncmdfailclientconnnotfoundrate	<Double>	Read-only	Rate (/s) counter for ngsconncmdfailclientconnnotfound
ngsicastart	<Double>	Read-only	Total number of ICA start
ngsicastartrate	<Double>	Read-only	Rate (/s) counter for ngsicastart
ngsicaend	<Double>	Read-only	Total number of ICA end
ngsicaendrate	<Double>	Read-only	Rate (/s) counter for ngsicaend
ngssocksapplaunchattempted	<Double>	Read-only	Total number of SOCKS app launch attempted

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ngssocksapplauncha ttemptedrate	<Double>	Read-only	Rate (/s) counter for ngssocksapplauncha ttempted
ngssocksapplaunchs uccess	<Double>	Read-only	Total number of SOCKS app launch success
ngssocksapplaunchs uccessrate	<Double>	Read-only	Rate (/s) counter for ngssocksapplaunchs uccess
ngscgpapplaunchatt empted	<Double>	Read-only	Total number of CGP app launch attempted
ngscgpapplaunchatt emptedrate	<Double>	Read-only	Rate (/s) counter for ngscgpapplaunchatt empted
ngscgpapplaunchsuc cess	<Double>	Read-only	Total number of CGP app launch success
ngscgpapplaunchsuc cessrate	<Double>	Read-only	Rate (/s) counter for ngscgpapplaunchsuc cess
ngsgctapplaunchatte mpted	<Double>	Read-only	Total number of GCT app launch attempted
ngsgctapplaunchatte mptedrate	<Double>	Read-only	Rate (/s) counter for ngsgctapplaunchatte mpted
ngsgctapplaunchsuc cess	<Double>	Read-only	Total number of GCT app launch success
ngsgctapplaunchsuc cessrate	<Double>	Read-only	Rate (/s) counter for ngsgctapplaunchsuc cess

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ngsstaapplaunchattempted	<Double>	Read-only	Total number of STA app launch attempted
ngsstaapplaunchattemptedrate	<Double>	Read-only	Rate (/s) counter for ngsstaapplaunchattempted
ngsstaapplaunchsuccess	<Double>	Read-only	Total number of STA app launch success
ngsstaapplaunchsuccessrate	<Double>	Read-only	Rate (/s) counter for ngsstaapplaunchsuccess
ngsedtle1secconnesttime	<Double>	Read-only	Total EDT connection with connect time less than 1 sec
ngsedtle1secconnesttimerate	<Double>	Read-only	Rate (/s) counter for ngsedtle1secconnesttime
ngsedtle2secconnesttime	<Double>	Read-only	Total EDT connection with connect time less than 2 sec
ngsedtle2secconnesttimerate	<Double>	Read-only	Rate (/s) counter for ngsedtle2secconnesttime
ngsedtle3secconnesttime	<Double>	Read-only	Total EDT connection with connect time less than 3 sec
ngsedtle3secconnesttimerate	<Double>	Read-only	Rate (/s) counter for ngsedtle3secconnesttime

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ngsedtle5secconnesttime	<Double>	Read-only	Total EDT connection with connect time less than 5 sec
ngsedtle5secconnesttimerate	<Double>	Read-only	Rate (/s) counter for ngsedtle5secconnesttime
ngsedtle8secconnesttime	<Double>	Read-only	Total EDT connection with connect time less than 8 sec
ngsedtle8secconnesttimerate	<Double>	Read-only	Rate (/s) counter for ngsedtle8secconnesttime
ngsedtgt8secconnesttime	<Double>	Read-only	Total EDT connection with connect time greater than 8 sec
ngsedtgt8secconnesttimerate	<Double>	Read-only	Rate (/s) counter for ngsedtgt8secconnesttime
ngsedtle1secclienthandshakeesttime	<Double>	Read-only	Total EDT handshake establishment time with client less than 1sec
ngsedtle1secclienthandshakeesttimerate	<Double>	Read-only	Rate (/s) counter for ngsedtle1secclienthandshakeesttime
ngsedtle2secclienthandshakeesttime	<Double>	Read-only	Total EDT handshake establishment time

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			with client less than 2sec
ngsedtle2secclienthandshakeesttimerate	<Double>	Read-only	Rate (/s) counter for ngsedtle2secclienthandshakeesttime
ngsedtle3secclienthandshakeesttime	<Double>	Read-only	Total EDT handshake establishment time with client less than 3sec
ngsedtle3secclienthandshakeesttimerate	<Double>	Read-only	Rate (/s) counter for ngsedtle3secclienthandshakeesttime
ngsedtgt3secclienthandshakeesttime	<Double>	Read-only	Total EDT handshake establishment time with client greater than 3sec
ngsedtgt3secclienthandshakeesttimerate	<Double>	Read-only	Rate (/s) counter for ngsedtgt3secclienthandshakeesttime
ngsedtle1secvdahandshakeesttime	<Double>	Read-only	Total EDT handshake establishment time with vda less than 1sec
ngsedtle1secvdahandshakeesttimerate	<Double>	Read-only	Rate (/s) counter for ngsedtle1secvdahandshakeesttime
ngsedtle2secvdahandshakeesttime	<Double>	Read-only	Total EDT handshake establishment time

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			with vda less than 2sec
ngsedtle2secvdahandshakeesttimerate	<Double>	Read-only	Rate (/s) counter for ngsedtle2secvdahandshakeesttime
ngsedtle3secvdahandshakeesttime	<Double>	Read-only	Total EDT handshake establishment time with vda less than 3sec
ngsedtle3secvdahandshakeesttimerate	<Double>	Read-only	Rate (/s) counter for ngsedtle3secvdahandshakeesttime
ngsedtgt3secvdahandshakeesttime	<Double>	Read-only	Total EDT handshake establishment time with vda greater than 3sec
ngsedtgt3secvdahandshakeesttimerate	<Double>	Read-only	Rate (/s) counter for ngsedtgt3secvdahandshakeesttime
ngsedtconnrequest	<Double>	Read-only	Total EDT connection request
ngsedtconnrequestrate	<Double>	Read-only	Rate (/s) counter for ngsedtconnrequest
ngsedtclientconnest	<Double>	Read-only	Total client EDT connection establishment
ngsedtclientconnestrate	<Double>	Read-only	Rate (/s) counter for ngsedtclientconnest
ngsedtnonrendzconnreqdrop	<Double>	Read-only	Total connect request drop due to

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			rendezvous not enabled
ngsedtnonrendzconnreqdroprate	<Double>	Read-only	Rate (/s) counter for ngsedtnonrendzconnreqdrop
ngsedtctrlsendconnfailure	<Double>	Read-only	Total send connect to controller failed
ngsedtctrlsendconnfailurerate	<Double>	Read-only	Rate (/s) counter for ngsedtctrlsendconnfailure
ngsedtapplaunchsuccess	<Double>	Read-only	Total EDT app launch success
ngsedtapplaunchsuccessrate	<Double>	Read-only	Rate (/s) counter for ngsedtapplaunchsuccess
ngsedtapplaunchfailure	<Double>	Read-only	Total EDT app launch failures
ngsedtapplaunchfailurerate	<Double>	Read-only	Rate (/s) counter for ngsedtapplaunchfailure
ngsedtstavalfailure	<Double>	Read-only	Total STA validation failures
ngsedtstavalfailurerate	<Double>	Read-only	Rate (/s) counter for ngsedtstavalfailure
ngsedtstavalsuccess	<Double>	Read-only	Total STA validation success
ngsedtstavalsuccessrate	<Double>	Read-only	Rate (/s) counter for ngsedtstavalsuccess
ngsedtfrvdaconn	<Double>	Read-only	Total FR VDA connection

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ngsedtfrvdaconnrate	<Double>	Read-only	Rate (/s) counter for ngsedtfrvdaconn
ngsedtfrsnconn	<Double>	Read-only	Total FR SN connection
ngsedtfrsnconnrate	<Double>	Read-only	Rate (/s) counter for ngsedtfrsnconn
ngsedtvdaconnest	<Double>	Read-only	Total VDA EDT connection establishment
ngsedtvdaconnestrate	<Double>	Read-only	Rate (/s) counter for ngsedtvdaconnest
ngsedtvdarendezvoustimeout	<Double>	Read-only	Total VDA rendezvous timeout
ngsedtvdarendezvoustimeoutrate	<Double>	Read-only	Rate (/s) counter for ngsedtvdarendezvoustimeout
ngsedtnonlossytunnel	<Double>	Read-only	Total EDT non lossy tunnels
ngsedtnonlossytunnelrate	<Double>	Read-only	Rate (/s) counter for ngsedtnonlossytunnel
ngsedtlossytunnel	<Double>	Read-only	Total EDT lossy tunnels
ngsedtlossytunnelrate	<Double>	Read-only	Rate (/s) counter for ngsedtlossytunnel
ngsedtgetrequestsenttoredis	<Double>	Read-only	Total Redis GET Request

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ngsedtgetrequestsenttoredisrate	<Double>	Read-only	Rate (/s) counter for ngsedtgetrequestsenttoredis
ngsedtredislookupsuccess	<Double>	Read-only	Total Redis lookup success
ngsedtredislookupsuccessrate	<Double>	Read-only	Rate (/s) counter for ngsedtredislookupsuccess
ngsedtredislookupfailure	<Double>	Read-only	Total Redis lookup failure
ngsedtredislookupfailurerate	<Double>	Read-only	Rate (/s) counter for ngsedtredislookupfailure
ngsedtredisentryadd succes	<Double>	Read-only	Entries Added To Redis Successfully
ngsedtredisentryadd succesrate	<Double>	Read-only	Rate (/s) counter for ngsedtredisentryadd succes
ngsedtredisentryaddfailure	<Double>	Read-only	Entries Addition to Redis failure
ngsedtredisentryaddfailurerate	<Double>	Read-only	Rate (/s) counter for ngsedtredisentryaddfailure
ngsedtredisentrydeletesuccess	<Double>	Read-only	Entry Deleted Successfully In Redis
ngsedtredisentrydeletesuccessrate	<Double>	Read-only	Rate (/s) counter for ngsedtredisentrydeletesuccess

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ngsedtredisentrydeletefailure	<Double>	Read-only	Entry Deletion Failed in Redis
ngsedtredisentrydeletefailurerate	<Double>	Read-only	Rate (/s) counter for ngsedtredisentrydeletefailure
ngsedttotsessionsreroutingdatapkt	<Double>	Read-only	Total EDT Sessions Re-Routing Data Pkt
ngsedtsessionsreroutingdatapktrate	<Double>	Read-only	Rate (/s) counter for ngsedttotsessionsreroutingdatapkt
ngsedttotsessionsreceivingredirectedpkt	<Double>	Read-only	Total EDT Sessions Receiving Redirected Pkt
ngsedtsessionsreceivingredirectedpktrate	<Double>	Read-only	Rate (/s) counter for ngsedttotsessionsreceivingredirectedpkt
ngsedtcurrentsessionsreroutingdatapkt	<Double>	Read-only	Current EDT Sessions Re-Routing Data Pkt
ngsedtcurrentsessionsreroutingdatapktrate	<Double>	Read-only	Rate (/s) counter for ngsedtcurrentsessionsreroutingdatapkt
ngsedtcurrentsessionsreceivingredirectedpkt	<Double>	Read-only	Current EDT Sessions Receiving Redirected Pkt
ngsedtcurrentsessionsreceivingredirectedpktrate	<Double>	Read-only	Rate (/s) counter for ngsedtcurrentsessionsreceivingredirectedpkt
ngsagentaccessle1secconnesttime	<Double>	Read-only	Total Agent Access based Connection

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			with connect time less than 1 sec
ngsagentaccessle1secconnesttimerate	<Double>	Read-only	Rate (/s) counter for ngsagentaccessle1secconnesttime
ngsagentaccessle2secconnesttime	<Double>	Read-only	Total Agent Access based Connection with connect time less than 2 sec
ngsagentaccessle2secconnesttimerate	<Double>	Read-only	Rate (/s) counter for ngsagentaccessle2secconnesttime
ngsagentaccessle3secconnesttime	<Double>	Read-only	Total Agent Access based Connection with connect time less than 3 sec
ngsagentaccessle3secconnesttimerate	<Double>	Read-only	Rate (/s) counter for ngsagentaccessle3secconnesttime
ngsagentaccessle5secconnesttime	<Double>	Read-only	Total Agent Access based Connection with connect time less than 5 sec
ngsagentaccessle5secconnesttimerate	<Double>	Read-only	Rate (/s) counter for ngsagentaccessle5secconnesttime
ngsagentaccessle8secconnesttime	<Double>	Read-only	Total Agent Access based Connection with connect time less than 8 sec
ngsagentaccessle8secconnesttimerate	<Double>	Read-only	Rate (/s) counter for ngsagentaccessle8secconnesttime

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ngsagentaccessle13 secconnesttime	<Double>	Read-only	Total Agent Access based Connection with connect time less than 13 sec
ngsagentaccessle13 secconnesttimerate	<Double>	Read-only	Rate (/s) counter for ngsagentaccessle13 secconnesttime
ngsagentaccessle21 secconnesttime	<Double>	Read-only	Total Agent Access based Connection with connect time less than 21 sec
ngsagentaccessle21 secconnesttimerate	<Double>	Read-only	Rate (/s) counter for ngsagentaccessle21 secconnesttime
ngsagentaccessgt21 secconnesttime	<Double>	Read-only	Total Agent Access based Connection with connect time greater than 21 sec
ngsagentaccessgt21 secconnesttimerate	<Double>	Read-only	Rate (/s) counter for ngsagentaccessgt21 secconnesttime

Operations

(click to see Properties)

- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/cloud **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/cloud? **args=detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get cloud resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/cloud? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "cloud": [ {

"ngsshieldle2secclxmtpconnesttimerate":<Double_value>,

"ngsedtapplaunchsuccess":<Double_value>,

"ngsapplaunchfailurerate":<Double_value>,

"ngsedtgetrequestsenttoredisrate":<Double_value>,

"ngsedtvdarendezvoustimeoutrate":<Double_value>,

"ngsshieldclxmtppubkeyvalfailurerate":<Double_value>,

"ngsedtapplaunchfailure":<Double_value>,

"ngsshielddemandedgwkeynotfound":<Double_value>,

"ngsedtvdarendezvoustimeout":<Double_value>,

"ngsedtcurrentsessionsreroutingdatapkt":<Double_value>,

"ngsagentaccessle21secconnesttimerate":<Double_value>,

"ngsedtle2secvdahandshakeesttime":<Double_value>,

"ngsedtcurrentsessionsreceivingredirectedpktrate":<Double_value>,

"ngsconncmdfailbyfr":<Double_value>,

"ngstunnelclosedbyvdarate":<Double_value>,

"ngsgctle1secconnesttime":<Double_value>,

"ngscgpapplaunchattemptedrate":<Double_value>,

"ngsedtredisentryaddsuccesrate":<Double_value>,
```

```
"ngsedtle2secclienthandshakeesttime":<Double_value>,

"ngstunnelclosedbyclient":<Double_value>,

"ngsshieldclxmtptrustestfailure":<Double_value>,

"ngsedttotsessionsreroutingdatapkt":<Double_value>,

"ngsshieldclxmtpconnestattemptedrate":<Double_value>,

"ngsshieldle5secclxmtpconnesttimerate":<Double_value>,

"ngsshieldakvgetsecretfailurerate":<Double_value>,

"ngsshieldawssmgetmastersecretfailure":<Double_value>,

"ngsedtsessionsreceivingredirectedpktrate":<Double_value>,

"ngsshieldgt21secclxmtpconnesttimerate":<Double_value>,

"ngsedtgt3secvdahandshakeesttime":<Double_value>,

"ngsedtclientconnest":<Double_value>,

"ngsle3secconnesttime":<Double_value>,

"ngsshieldclxmtpconnestsuccessrate":<Double_value>,

"ngsconncmdfailclientconnnotfoundrate":<Double_value>,

"ngssocksapplaunchsuccessrate":<Double_value>,

"ngsedtle3secvdahandshakeesttimerate":<Double_value>,

"ngsle3secconnesttimerate":<Double_value>,

"ngsgctle8secconnesttime":<Double_value>,

"ngsshieldclxmtpallowtargetrate":<Double_value>,

"ngsedtstavalsuccessrate":<Double_value>,

"ngsshieldawssmgetmastersecretfailurerate":<Double_value>,
```

```
"ngsedtredisentrydeletesuccess":<Double_value>,

"ngsshieldawssmgetsecretfailurerate":<Double_value>,

"ngsshieldclxmtpconnvalidationfailurerate":<Double_value>,

"ngsedtlossytunnel":<Double_value>,

"ngsicastart":<Double_value>,

"ngsedtcurrentsessionsreroutingdatapktrate":<Double_value>,

"ngsedtfrvdaconn":<Double_value>,

"ngsshieldcldecryptionfailure":<Double_value>,

"ngsshieldclxmtppubkeyvalfailure":<Double_value>,

"ngsshieldclxmtpredirecttargetrate":<Double_value>,

"ngsedtapplaunchfailurerate":<Double_value>,

"ngsedtle1secvdahandshakeesttimerate":<Double_value>,

"ngstunnelclosedbyvda":<Double_value>,

"ngscgpapplaunchsuccess":<Double_value>,

"ngsagentaccessle2secconnesttimerate":<Double_value>,

"ngsgctgt8secconnesttime":<Double_value>,

"ngsrendezvousv2delayedresponserate":<Double_value>,

"ngsrendezvousv2fallbacktov1rate":<Double_value>,

"ngsagentaccessle5secconnesttimerate":<Double_value>,

"ngsedtredislookupfailure":<Double_value>,

"ngsgctgt8secconnesttimerate":<Double_value>,

"ngsconncmdfailclientconnnotfound":<Double_value>,
```

```
"ngsshieldfanout":<Double_value>,

"ngsshieldclxmtpdeny":<Double_value>,

"ngsshieldakvtokenfailure":<Double_value>,

"ngsedtle2secvdahandshakeesttimerate":<Double_value>,

"ngsshieldawssmtokenfailure":<Double_value>,

"ngsrendezvousv1launchfailure":<Double_value>,

"ngsagentaccessle3secconnesttime":<Double_value>,

"ngsrendezvousv1sntcntcmdfailurerate":<Double_value>,

"ngsedtle8secconnesttime":<Double_value>,

"ngsapplaunchsuccess":<Double_value>,

"ngsshieldcldecryptionfailurerate":<Double_value>,

"ngsrendezvousv2invalidcapabilityrate":<Double_value>,

"ngsedtapplaunchsuccessrate":<Double_value>,

"ngsedtsessionsreroutingdatapktrate":<Double_value>,

"ngsedtredislookupsuccessrate":<Double_value>,

"ngsagentaccessle5secconnesttime":<Double_value>,

"ngsagentaccessle8secconnesttime":<Double_value>,

"ngsagentaccessle13secconnesttime":<Double_value>,

"ngsstavalfailure":<Double_value>,

"ngssocksapplaunchattempted":<Double_value>,

"ngsedtredisentrydeletefailure":<Double_value>,

"ngsshieldle3secclxmtpconnesttime":<Double_value>,
```

```
"ngsgctapplaunchattemptedrate":<Double_value>,

"ngsedtgt8secconnesttime":<Double_value>,

"ngsshielddemandedgwkeynotfoundrate":<Double_value>,

"ngsedttotsessionsreceivingredirectedpkt":<Double_value>,

"ngsedtle8secconnesttimerate":<Double_value>,

"ngsrendezvousv2launchsuccess":<Double_value>,

"ngsshieldle1secclxmtpconnesttime":<Double_value>,

"ngsstavalfailurerate":<Double_value>,

"ngsstaapplaunchattempted":<Double_value>,

"ngstunnelclosedbyclientrate":<Double_value>,

"ngsapplaunchattemptedrate":<Double_value>,

"ngsedtnonrendzconnreqdroprate":<Double_value>,

"ngsgctapplaunchsuccessrate":<Double_value>,

"ngsticketsvcdownrate":<Double_value>,

"ngsedtstavalfailure":<Double_value>,

"ngsedtle1secconnesttime":<Double_value>,

"ngsshieldle8secclxmtpconnesttime":<Double_value>,

"ngsgctle8secconnesttimerate":<Double_value>,

"ngsrendezvousv1launchfailurerate":<Double_value>,

"ngsedtnonrendzconnreqdrop":<Double_value>,

"ngsedtvdaconnest":<Double_value>,

"ngsshieldkeycacheemptyrate":<Double_value>,
```

```
"ngsshieldclxmtptrustestfailurerate":<Double_value>,

"ngsticketsvcdown":<Double_value>,

"ngsshieldclxmtpcompleterate":<Double_value>,

"ngssocksapplaunchsuccess":<Double_value>,

"ngsrendezvousv2launchsuccessrate":<Double_value>,

"ngsgctapplaunchsuccess":<Double_value>,

"ngsedtvdaconnestrate":<Double_value>,

"ngsshieldclxmtpconnestattempted":<Double_value>,

"ngsshieldclxmtpcomplete":<Double_value>,

"ngscgpapplaunchsuccessrate":<Double_value>,

"ngsagentaccessle1secconnesttimerate":<Double_value>,

"ngsshieldakvgetsecretlistfailure":<Double_value>,

"ngsstavalsuccessrate":<Double_value>,

"ngsshieldclxmtpauthorizeconnreqfailurerate":<Double_value>,

"ngsshieldawssmgetsecretfailure":<Double_value>,

"ngsshieldclxmtpconnectorfanouttimeoutrate":<Double_value>,

"ngsshieldkeyfetchfailurerate":<Double_value>,

"ngsgctle1secconnesttimerate":<Double_value>,

"ngsstavalsuccess":<Double_value>,

"ngsshielddemandedcliskeynotfound":<Double_value>,

"ngsedtlossytunnelrate":<Double_value>,

"ngsagentaccessle8secconnesttimerate":<Double_value>,
```

```
"ngsedtredisentrydeletefailurerate":<Double_value>,

"ngsdelayedconnectorresponse":<Double_value>,

"ngsconncmdfailbyfrrate":<Double_value>,

"ngsedtle1secclienthandshakeesttimerate":<Double_value>,

"ngsedtfrvdaconnrate":<Double_value>,

"ngsedtgt3secclienthandshakeesttime":<Double_value>,

"ngsshieldle13secclxmtpconnesttimerate":<Double_value>,

"ngsrendezvousv1sntcntcmdfailure":<Double_value>,

"ngsagentaccessle13secconnesttimerate":<Double_value>,

"ngsshieldle3secclxmtpconnesttimerate":<Double_value>,

"ngsedtredisentryaddfailurerate":<Double_value>,

"ngsle5secconnesttime":<Double_value>,

"ngsrendezvousv1launchsuccessrate":<Double_value>,

"ngsedtfrsnconnrate":<Double_value>,

"ngsapplaunchsuccessrate":<Double_value>,

"ngsedtle5secconnesttimerate":<Double_value>,

"ngsedtnonlossytunnelrate":<Double_value>,

"ngsapplaunchattempted":<Double_value>,

"ngsshieldle1secclxmtpconnesttimerate":<Double_value>,

"ngsshielddemandedcliskeynotfoundrate":<Double_value>,

"ngsshieldclvalidationfailure":<Double_value>,

"ngsedtle5secconnesttime":<Double_value>,
```

```
"ngsshieldclxmtpdenyrate":<Double_value>,

"ngsgctle2secconnesttimerate":<Double_value>,

"ngsshieldle5secclxmtpconnesttime":<Double_value>,

"ngsgctle5secconnesttimerate":<Double_value>,

"ngsedtconnrequestrate":<Double_value>,

"ngsedtle3secclienthandshakeesttimerate":<Double_value>,

"ngsagentaccessgt21secconnesttime":<Double_value>,

"ngsedtgt3secvdahandshakeesttimerate":<Double_value>,

"ngsedtnonlossytunnel":<Double_value>,

"ngsedtctrlsendconnfailurerate":<Double_value>,

"ngsshieldclvalidationfailurerate":<Double_value>,

"ngsrendezvousv2sntcntcmdfailure":<Double_value>,

"ngsedtredislookupfailurerate":<Double_value>,

"ngsedtredisentrydeletesuccessrate":<Double_value>,

"ngsgctle3secconnesttime":<Double_value>,

"ngsedtredisentryaddfailure":<Double_value>,

"ngsstaapplaunchsuccessrate":<Double_value>,

"ngsshieldawssmtokenfailurerate":<Double_value>,

"ngsagentaccessgt21secconnesttimerate":<Double_value>,

"ngsshielddemandedrtkeynotfound":<Double_value>,

"ngsle5secconnesttimerate":<Double_value>,

"ngsgctle2secconnesttime":<Double_value>,
```

```
"ngsshieldclxmtpsoftdenyrate":<Double_value>,

"ngscgpapplaunchattempted":<Double_value>,

"ngsedtctrlsendconnfailure":<Double_value>,

"ngsshieldclxmtpsoftdeny":<Double_value>,

"ngsrendezvousv2launchfailurerate":<Double_value>,

"ngsshieldle2secclxmtpconnesttime":<Double_value>,

"ngsedtstavalfailurerate":<Double_value>,

"ngssocksapplaunchattemptedrate":<Double_value>,

"ngsedtle1secconnesttimerate":<Double_value>,

"ngsshieldclxmtpallowtarget":<Double_value>,

"ngsshieldclxmtpglobalfanouttimeoutrate":<Double_value>,

"ngsedtclientconnestrate":<Double_value>,

"ngsedtle3secconnesttime":<Double_value>,

"ngsshieldclxmtpglobalfanouttimeout":<Double_value>,

"ngsicastartrate":<Double_value>,

"ngsrendezvousv1launchsuccess":<Double_value>,

"ngsshieldle8secclxmtpconnesttimerate":<Double_value>,

"ngsrendezvousv2sntcntcmdfailurerate":<Double_value>,

"ngsle8secconnesttimerate":<Double_value>,

"ngsgt8secconnesttimerate":<Double_value>,

"ngsedtgt3secclienthandshakeesttimerate":<Double_value>,

"ngsshieldakvgetsecretfailure":<Double_value>,
```

```
"ngsicaend":<Double_value>,

"ngsedtredisentryaddsucces":<Double_value>,

"ngsgctle3secconnesttimerate":<Double_value>,

"ngsagentaccessle2secconnesttime":<Double_value>,

"ngsle2secconnesttime":<Double_value>,

"ngsedtredislookupsuccess":<Double_value>,

"ngsedtle3secconnesttimerate":<Double_value>,

"ngsedtle3secclienthandshakeesttime":<Double_value>,

"ngsshieldclxmtpconnestsuccess":<Double_value>,

"ngsedtgetrequestsenttoredis":<Double_value>,

"ngsdelayedconnectorresponserate":<Double_value>,

"ngsedtle2secconnesttime":<Double_value>,

"ngsstaapplaunchattemptedrate":<Double_value>,

"ngsshieldle21secclxmtpconnesttimerate":<Double_value>,

"ngsstaapplaunchsuccess":<Double_value>,

"ngsle1secconnesttime":<Double_value>,

"ngsshieldle21secclxmtpconnesttime":<Double_value>,

"ngsapplaunchfailure":<Double_value>,

"ngsrendezvousv2invalidcapability":<Double_value>,

"ngsedtle1secvdahandshakeesttime":<Double_value>,

"ngsshieldgt21secclxmtpconnesttime":<Double_value>,

"ngsshieldclxmtpauthorizeconnreqfailure":<Double_value>,
```

```
"ngsicaendrate":<Double_value>,

"ngsedtgt8secconnesttimerate":<Double_value>,

"ngsedtle1secclienthandshakeesttime":<Double_value>,

"ngsshieldclxmtpconnectorfanouttimeout":<Double_value>,

"ngsagentaccessle21secconnesttime":<Double_value>,

"ngsrendezvousv2launchfailure":<Double_value>,

"ngsedtcurrentsessionsreceivingredirectedpkt":<Double_value>,

"ngsshieldakvgetsecretlistfailurerate":<Double_value>,

"ngsle1secconnesttimerate":<Double_value>,

"ngsle2secconnesttimerate":<Double_value>,

"ngsshieldle13secclxmtpconnesttime":<Double_value>,

"ngsgctapplaunchattempted":<Double_value>,

"ngsshielddemandedrtkeynotfoundrate":<Double_value>,

"ngsshieldclxmtpredirecttarget":<Double_value>,

"ngsrendezvousv2delayedresponse":<Double_value>,

"ngsshieldkeycacheempty":<Double_value>,

"ngsedtconnrequest":<Double_value>,

"ngsgctle5secconnesttime":<Double_value>,

"ngsgt8secconnesttime":<Double_value>,

"ngsedtfrsnconn":<Double_value>,

"ngsshieldclxmtpconnvalidationfailure":<Double_value>,

"ngsagentaccessle3secconnesttimerate":<Double_value>,
```

```
"ngsedtle2secclienthandshakeesttimerate":<Double_value>,

"ngsedtstavalsuccess":<Double_value>,

"ngsrendezvousv2fallbacktov1":<Double_value>,

"ngsedtle2secconnesttimerate":<Double_value>,

"ngsagentaccessle1secconnesttime":<Double_value>,

"ngsshieldfanoutrate":<Double_value>,

"ngsle8secconnesttime":<Double_value>,

"ngsedtle3secvdahandshakeesttime":<Double_value>,

"ngsshieldkeyfetchfailure":<Double_value>,

"ngsshieldakvtokenfailurerate":<Double_value>

}]}
```


cluster

Cluster

Cluster commands.

NAME	DESCRIPTION
clusterinstance	Statistics for cluster instance resource.
clusternode	Statistics for cluster node resource.

clusterinstance

Statistics for cluster instance resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
clid	<Integer>	Read-write	ID of the cluster instance for which to display statistics. Minimum value = 1 Maximum value = 128
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full
clbkplanetx	<Double>	Read-only	Traffic transmitted from backplane (in mbits)
clbkplanetxrate	<Double>	Read-only	Rate (/s) counter for clbkplanetx
clbkplanerx	<Double>	Read-only	Traffic received on backplane (in mbits)
clbkplanerxrate	<Double>	Read-only	Rate (/s) counter for clbkplanerx
clnumnodes	<Double>	Read-only	Number of nodes in the cluster.
clcurstatus	<String>	Read-only	State of the cluster.
clviewleader	<String>	Read-only	NSIP address of the Configuration Coordinator of the cluster.
totsteeredpkts	<Double>	Read-only	Total number of packets steered on

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			the cluster backplane.
steeredpktsrate	<Double>	Read-only	Rate (/s) counter for totsteeredpkts
numdfddroppkts	<Double>	Read-only	Number of steered packets that are dropped.
totpropagationtimeout	<Double>	Read-only	Number of times the update to the client timed-out.

Operations

(click to see Properties)

- GET (ALL)
- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/clusterinstance **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/clusterinstance? **args=clid: <Integer_value> ,detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get clusterinstance resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/clusterinstance? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "clusterinstance": [ {

"clid":<Integer_value>,

"clbkplanerx":<Double_value>,
```

```
"clbkplanetx":<Double_value>,

"numdfddroppkts":<Double_value>,

"totsteeredpkts":<Double_value>,

"clviewleader":<String_value>,

"clnumnodes":<Double_value>,

"totpropagationtimeout":<Double_value>,

"steeredpktsrate":<Double_value>,

"clbkplanerxrate":<Double_value>,

"clcurstatus":<String_value>,

"clbkplanetxrate":<Double_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/stat/clusterinstance/ clid_value><Integer> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "clusterinstance": [ {

"clid":<Integer_value>,

"clbkplanerx":<Double_value>,

"clbkplanetx":<Double_value>,

"numdfddroppkts":<Double_value>,

"totsteeredpkts":<Double_value>,

"clviewleader":<String_value>,

"clnumnodes":<Double_value>,

"totpropagationtimeout":<Double_value>,

"steeredpktsrate":<Double_value>,

"clbkplanerxrate":<Double_value>,

"clcurstatus":<String_value>,

"clbkplanetxrate":<Double_value>

}]}
```

clusternode

Statistics for cluster node resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
nodeid	<Integer>	Read-write	ID of the cluster node for which to display statistics. If an ID is not provided,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			statistics are shown for all nodes. Minimum value = 0 Maximum value = 31
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full
clsyncstate	<String>	Read-only	Sync state of the cluster node.
clnodeeffectivehealth	<String>	Read-only	Health of the cluster node.
clnodeip	<String>	Read-only	NSIP address of the cluster node.
clmasterstate	<String>	Read-only	Operational state of the cluster node.
cltothbtx	<Double>	Read-only	Number of heartbeats sent. When executed from the NSIP address, shows the statistics for local node only. For remote node it shows a value of 0. When executed from the cluster IP address, shows all the statistics.
cltothbrx	<Double>	Read-only	Number of heartbeats received. When executed from the NSIP address,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			shows the statistics for local node only. For remote node it shows a value of 0. When executed from the cluster IP address, shows all the statistics.
nnmcurconn	<Double>	Read-only	Number of connections open for node-to-node communication.
nnmtotconntx	<Double>	Read-only	Number of node-to-node messages sent. When executed from the NSIP address, shows the statistics for local node only. For remote node it shows a value of 0. When executed from the cluster IP address, shows all the statistics.
nnmtotconnrx	<Double>	Read-only	Number of node-to-node messages received. When executed from the NSIP address, shows the statistics for local node only. For remote node it shows a value of 0. When executed from the cluster IP address, shows all the statistics.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
clptpstate	<String>	Read-only	PTP state of the node. This state is Master for one node and Slave for the rest. When executed from the NSIP address, shows the statistics for local node only. For remote node it shows UNKNOWN. When executed from the cluster IP address, shows all the statistics.
clptptx	<Double>	Read-only	Number of PTP packets transmitted by the node. When executed from the NSIP address, shows the statistics for local node only. For remote node it shows a value of 0. When executed from the cluster IP address, shows all the statistics.
clptprx	<Double>	Read-only	Number of PTP packets received on the node. When executed from the NSIP address, shows the statistics for local node only. For remote node it shows a value of 0. When executed from the cluster IP

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			address, shows all the statistics.
nnmerrmsend	<Double>	Read-only	Number of errors in sending node-to-node multicast/ broadcast messages. When executed from the NSIP address, shows the statistics for local node only. For remote node it shows a value of 0. When executed from the cluster IP address, shows all the statistics.

Operations

(click to see Properties)

- GET (ALL)
- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/clusternode **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/clusternode? **args=nodeid: <Integer_value> ,detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get clusternode resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/clusternode? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "clusternode": [ {

"nodeid":<Integer_value>,

"cltothbtx":<Double_value>,

"nnmtotconnrx":<Double_value>,

"nnmtotconntx":<Double_value>,

"cltothbrx":<Double_value>,

"clnodeeffectivehealth":<String_value>,

"clptprx":<Double_value>,

"nnmerrmsend":<Double_value>,

"clptptx":<Double_value>,

"clnodeip":<String_value>,

"clptpstate":<String_value>,

"nnmcurconn":<Double_value>,

"clmasterstate":<String_value>,

"clsyncstate":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/stat/clusternode/ nodeid_value><Integer> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "clusternode": [ {

"nodeid":<Integer_value>,

"cltothbtx":<Double_value>,

"nnmtotconnrx":<Double_value>,

"nnmtotconntx":<Double_value>,

"cltothbrx":<Double_value>,

"clnodeeffectivehealth":<String_value>,

"clptprx":<Double_value>,

"nnmerrmsend":<Double_value>,

"clptptx":<Double_value>,

"clnodeip":<String_value>,

"clptpstate":<String_value>,

"nnmcurconn":<Double_value>,

"clmasterstate":<String_value>,

"clsyncstate":<String_value>

}]}
```

cmp

Compression

Compression statistics. The system's feature for compressing HTTP responses to compression-aware browsers.

NAME	DESCRIPTION
cmp	Statistics for cmp.
cmppolicy	Statistics for compression policy resource.
cmppolicylabel	Statistics for compression policy label resource.

cmp

Statistics for cmp.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full
delbwsaving	<Double>	Read-only	Bandwidth saving from delta compression expressed as percentage.
delcmpratio	<Double>	Read-only	Ratio of compressible data

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			received to compressed data transmitted.If this ratio is one (uncmp:1.0) that means compression is disabled or we are not able to compress even a single compressible packet.
decomptcpratio	<Double>	Read-only	Ratio of decompressed data transmitted to compressed data received.
decomptcpbandwidthsaving	<Double>	Read-only	Bandwidth saving from TCP compression expressed as percentage.
comptcpratio	<Double>	Read-only	Ratio of compressible data received to compressed data transmitted.If this ratio is one (uncmp:1.0) that means compression is disabled or we are not able to compress even a single compressible packet.
comptcpbandwidthsaving	<Double>	Read-only	Bandwidth saving from TCP compression expressed as percentage.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
comptotaldatacompressionratio	<Double>	Read-only	Ratio of total HTTP data received to total HTTP data transmitted.
comphttpbandwidthsaving	<Double>	Read-only	Bandwidth saving from TCP compression expressed as percentage.
compratio	<Double>	Read-only	Ratio of the compressible data received from the server to the compressed data sent to the client.
comptotalrequests	<Double>	Read-only	Number of HTTP compression requests the Citrix ADC receives for which the response is successfully compressed. For example, after you enable compression and configure services, if you send HTTP requests to the Citrix ADC using a HTTP client that supports compression, and Citrix ADC compresses the corresponding response, this counter is incremented.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
comprequestsrate	<Double>	Read-only	Rate (/s) counter for comptotalrequests
comptotalrxbytes	<Double>	Read-only	Number of bytes that can be compressed, which the Citrix ADC receives from the server. This gives the content length of the response that the Citrix ADC receives from server.
comprxbytesrate	<Double>	Read-only	Rate (/s) counter for comptotalrxbytes
comptotaltxbytes	<Double>	Read-only	Number of bytes the Citrix ADC sends to the client after compressing the response from the server.
comptxbytesrate	<Double>	Read-only	Rate (/s) counter for comptotaltxbytes
comptotalrxpackets	<Double>	Read-only	Number of HTTP packets that can be compressed, which the Citrix ADC receives from the server.
comprxpacketsrate	<Double>	Read-only	Rate (/s) counter for comptotalrxpackets
comptotaltxpackets	<Double>	Read-only	Number of HTTP packets that the Citrix ADC sends to the client after compressing the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			response from the server.
comptxpacketsrate	<Double>	Read-only	Rate (/s) counter for comptotaltxpackets
comptcptotalrxbytes	<Double>	Read-only	Number of bytes that can be compressed, which the Citrix ADC receives from the server. This gives the content length of the response that the Citrix ADC receives from server.
comptcprxbytesrate	<Double>	Read-only	Rate (/s) counter for comptcptotalrxbytes
comptcptotalrxpackets	<Double>	Read-only	Total number of compressible packets received by Citrix ADC.
comptcprxpacketsrate	<Double>	Read-only	Rate (/s) counter for comptcptotalrxpackets
comptcptotaltxbytes	<Double>	Read-only	Number of bytes that the Citrix ADC sends to the client after compressing the response from the server.
comptcptxbytesrate	<Double>	Read-only	Rate (/s) counter for comptcptotaltxbytes
comptcptotaltxpackets	<Double>	Read-only	Number of TCP packets that the Citrix ADC sends to the client after

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			compressing the response from the server.
comptcptxpacketsrate	<Double>	Read-only	Rate (/s) counter for comptcptotaltxpackets
comptcptotalquantum	<Double>	Read-only	Number of times the Citrix ADC compresses a quantum of data. Citrix ADC buffers the data received from the server till it reaches the quantum size and then compresses the buffered data and transmits to the client.
comptcpquantumrate	<Double>	Read-only	Rate (/s) counter for comptcptotalquantum
comptcptotalpush	<Double>	Read-only	Number of times the Citrix ADC compresses data on receiving a TCP PUSH flag from the server. The PUSH flag ensures that data is compressed immediately without waiting for the buffered data size to reach the quantum size.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
comptcppushrate	<Double>	Read-only	Rate (/s) counter for comptcptotalpush
comptcptotaleoi	<Double>	Read-only	Number of times the Citrix ADC compresses data on receiving End Of Input (FIN packet). When the Citrix ADC receives End Of Input (FIN packet), it compresses the buffered data immediately without waiting for the buffered data size to reach the quantum size.
comptcpeoirate	<Double>	Read-only	Rate (/s) counter for comptcptotaleoi
comptcptotaltimer	<Double>	Read-only	Number of times the Citrix ADC compresses data on expiration of data accumulation timer. The timer expires if the server response is very slow and consequently, the Citrix ADC does not receive response for a certain amount of time. Under such a condition, the Citrix ADC compresses the buffered data immediately without waiting for the buffered data size to

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			reach the quantum size.
comptcptimerrate	<Double>	Read-only	Rate (/s) counter for comptcptotaltimer
decomptcprxbytes	<Double>	Read-only	Total number of compressed bytes received by Citrix ADC.
decomptcprxbytesrate	<Double>	Read-only	Rate (/s) counter for decomptcprxbytes
decomptcprxpackets	<Double>	Read-only	Total number of compressed packets received by Citrix ADC.
decomptcprxpacketsrate	<Double>	Read-only	Rate (/s) counter for decomptcprxpackets
decomptcptxbytes	<Double>	Read-only	Total number of decompressed bytes transmitted by Citrix ADC.
decomptcptxbytesrate	<Double>	Read-only	Rate (/s) counter for decomptcptxbytes
decomptcptxpackets	<Double>	Read-only	Total number of decompressed packets transmitted by Citrix ADC.
decomptcptxpacketsrate	<Double>	Read-only	Rate (/s) counter for decomptcptxpackets
decomptcperrdata	<Double>	Read-only	Number of data errors encountered while decompressing.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
decomptcperrdatarate	<Double>	Read-only	Rate (/s) counter for decomptcperrdata
decomptcperrlessdata	<Double>	Read-only	Number of times Citrix ADC received less data than declared by protocol.
decomptcperrlessdatarate	<Double>	Read-only	Rate (/s) counter for decomptcperrlessdata
decomptcperrmoredata	<Double>	Read-only	Number of times Citrix ADC received more data than declared by protocol.
decomptcperrmoredatarate	<Double>	Read-only	Rate (/s) counter for decomptcperrmoredata
decomptcperrmemory	<Double>	Read-only	Number of times memory failures occurred while decompressing.
decomptcperrmemoryrate	<Double>	Read-only	Rate (/s) counter for decomptcperrmemory
decomptcperrunknown	<Double>	Read-only	Number of times unknown errors occurred while decompressing.
decomptcperrunknownrate	<Double>	Read-only	Rate (/s) counter for decomptcperrunknown
delcomptotalrequests	<Double>	Read-only	Total number of delta compression

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			requests received by Citrix ADC.
delcomprequestsrate	<Double>	Read-only	Rate (/s) counter for delcomptotalrequests
delcompdone	<Double>	Read-only	Total number of delta compressions done by Citrix ADC.
delcompdonerate	<Double>	Read-only	Rate (/s) counter for delcompdone
delcomptcprxbytes	<Double>	Read-only	Total number of delta-compressible bytes received by Citrix ADC.
delcomptcprxbytesrate	<Double>	Read-only	Rate (/s) counter for delcomptcprxbytes
delcomptcptxbytes	<Double>	Read-only	Total number of delta-compressed bytes transmitted by Citrix ADC.
delcomptcptxbytesrate	<Double>	Read-only	Rate (/s) counter for delcomptcptxbytes
delcompfirstaccess	<Double>	Read-only	Total number of delta compression first accesses.
delcompfirstaccessrate	<Double>	Read-only	Rate (/s) counter for delcompfirstaccess
delcomptcprxpackets	<Double>	Read-only	Number of delta-compressible packets received.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
delcomptcprxpackets rate	<Double>	Read-only	Rate (/s) counter for delcomptcprxpackets
delcomptcptxpackets	<Double>	Read-only	Total number of delta-compressed packets transmitted by Citrix ADC.
delcomptcptxpackets rate	<Double>	Read-only	Rate (/s) counter for delcomptcptxpackets
delcompbaseserved	<Double>	Read-only	Total number of basefile requests served by Citrix ADC.
delcompbaseservedr ate	<Double>	Read-only	Rate (/s) counter for delcompbaseserved
delcompbasetcptxbyt es	<Double>	Read-only	Number of basefile bytes transmitted by Citrix ADC.
delcompbasetcptxbyt esrate	<Double>	Read-only	Rate (/s) counter for delcompbasetcptxbyt es
delcomperrbypassed	<Double>	Read-only	Number of times delta-compression bypassed by Citrix ADC.
delcomperrbypassed rate	<Double>	Read-only	Rate (/s) counter for delcomperrbypassed
delcomperrbfilewhdrf ailed	<Double>	Read-only	Number of times basefile could not be updated in Citrix ADC cache.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
delcomperrbfilewhdrfailedrate	<Double>	Read-only	Rate (/s) counter for delcomperrbfilewhdrfailed
delcomperrnostoremiss	<Double>	Read-only	Number of times basefile was not found in Citrix ADC cache.
delcomperrnostoremissrate	<Double>	Read-only	Rate (/s) counter for delcomperrnostoremiss
delcomperrreqinfotoobig	<Double>	Read-only	Number of times basefile request URL was too large.
delcomperrreqinfotoobigrate	<Double>	Read-only	Rate (/s) counter for delcomperrreqinfotoobig
delcomperrreqinfoallocfail	<Double>	Read-only	Number of times requested basefile could not be allocated.
delcomperrreqinfoallocfailrate	<Double>	Read-only	Rate (/s) counter for delcomperrreqinfoallocfail
delcomperrsessallocfail	<Double>	Read-only	Number of times delta compression session could not be allocated.
delcomperrsessallocfailrate	<Double>	Read-only	Rate (/s) counter for delcomperrsessallocfail

Operations

(click to see Properties)

- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/cmp **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/cmp? **args=detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get cmp resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/cmp? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "cmp": [ {

"comptcpbandwidthsaving":<Double_value>,

"comptcprxbytesrate":<Double_value>,

"decomptcperrlessdata":<Double_value>,

"delcomptcptxbytesrate":<Double_value>,

"decomptcperrmemory":<Double_value>,

"delcomptcptxpacketsrate":<Double_value>,

"decomptcperrunknown":<Double_value>,

"delcomperrsessallocfailrate":<Double_value>,

"delcompfirstaccessrate":<Double_value>,

"comptxpacketsrate":<Double_value>,

"delcompbaseserved":<Double_value>,

"delcomperrnostoremissrate":<Double_value>,

"delcomptcprxbytes":<Double_value>,
```

```
"delcompdone":<Double_value>,

"comprxpacketsrate":<Double_value>,

"decomptcperrlessdatarate":<Double_value>,

"comptcptxbytesrate":<Double_value>,

"comprxbytesrate":<Double_value>,

"decomptcptxpackets":<Double_value>,

"comptotaltxpackets":<Double_value>,

"comptotalrxpackets":<Double_value>,

"decomptcprxpackets":<Double_value>,

"delcomperrreqinfoallocfail":<Double_value>,

"comprequestsrate":<Double_value>,

"comptotaldatacompressionratio":<Double_value>,

"delcomptcptxbytes":<Double_value>,

"comptxbytesrate":<Double_value>,

"comptcptotaltxpackets":<Double_value>,

"delbwsaving":<Double_value>,

"delcomperrbypassed":<Double_value>,

"delcomptcprxpacketsrate":<Double_value>,

"comptcpratio":<Double_value>,

"comptcpquantumrate":<Double_value>,

"delcomperrbfilewhdrfailedrate":<Double_value>,

"comptcptotalrxpackets":<Double_value>,
```

```
"decomptcpbandwidthsaving":<Double_value>,

"delcomperrreqinfoallocfailrate":<Double_value>,

"comptcptotalpush":<Double_value>,

"decomptcperrdata":<Double_value>,

"delcompbaseservedrate":<Double_value>,

"comptcptimerrate":<Double_value>,

"delcomptcprxbytesrate":<Double_value>,

"decomptcperrdatarate":<Double_value>,

"delcomperrsessallocfail":<Double_value>,

"comphttpbandwidthsaving":<Double_value>,

"delcomperrnostoremiss":<Double_value>,

"decomptcperrmemoryrate":<Double_value>,

"comptcptotalrxbytes":<Double_value>,

"delcomperrreqinfotoobigrate":<Double_value>,

"comptcptotaltxbytes":<Double_value>,

"decomptcperrmoredata":<Double_value>,

"delcompfirstaccess":<Double_value>,

"delcomperrreqinfotoobig":<Double_value>,

"delcomperrbfilewhdrfailed":<Double_value>,

"comptotalrequests":<Double_value>,

"decomptcperrmoredatarate":<Double_value>,

"delcompbasetcptxbytes":<Double_value>,
```

```
"delcomptcprxpackets":<Double_value>,

"comptcprxpacketsrate":<Double_value>,

"comptcptotalquantum":<Double_value>,

"decomptcptxpacketsrate":<Double_value>,

"decomptcprxpacketsrate":<Double_value>,

"decomptcperrunknownrate":<Double_value>,

"delcomptcptxpackets":<Double_value>,

"delcomprequestsrate":<Double_value>,

"comptcppushrate":<Double_value>,

"comptcptotaltimer":<Double_value>,

"comptcptotaleoi":<Double_value>,

"delcompdonerate":<Double_value>,

"delcmpratio":<Double_value>,

"delcompbasetcptxbytesrate":<Double_value>,

"decomptcpratio":<Double_value>,

"comptcpeoirate":<Double_value>,

"delcomperrbypassedrate":<Double_value>,

"compratio":<Double_value>,

"comptotalrxbytes":<Double_value>,

"decomptcprxbytes":<Double_value>,

"decomptcptxbytes":<Double_value>,

"comptotaltxbytes":<Double_value>,
```

```
"comptcptxpacketsrate":<Double_value>,

"decomptcprxbytesrate":<Double_value>,

"delcomptotalrequests":<Double_value>,

"decomptcptxbytesrate":<Double_value>

}]}
```

cmppolicy

Statistics for compression policy resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the compression policy for which to display statistics. If no name is specified, statistics for all compression polices are shown. Minimum length = 1
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full
pipolicyhits	<Double>	Read-only	Number of hits on the policy
pipolicyhitsrate	<Double>	Read-only	Rate (/s) counter for pipolicyhits

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
pipolicyundefhits	<Double>	Read-only	Number of undef hits on the policy
pipolicyundefhitsrate	<Double>	Read-only	Rate (/s) counter for pipolicyundefhits

Operations

(click to see Properties)

- GET (ALL)
- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/cmppolicy **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/cmppolicy? **args=name: <String_value> ,detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get cmppolicy resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/cmppolicy? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "cmppolicy": [ {

"name":<String_value>,

"pipolicyhits":<Double_value>,

"pipolicyundefhits":<Double_value>,

"pipolicyhitsrate":<Double_value>,

"pipolicyundefhitsrate":<Double_value>
```

```
}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/stat/cmppolicy/ name_value><String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "cmppolicy": [ {

"name":<String_value>,

"pipolicyhits":<Double_value>,

"pipolicyundefhits":<Double_value>,

"pipolicyhitsrate":<Double_value>,

"pipolicyundefhitsrate":<Double_value>

}]}
```

cmppolicylabel

Statistics for compression policy label resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
labelname	<String>	Read-write	Name of the compression policy label for which to display statistics. If not specified, statistics are displayed for all compression policy labels. Minimum length = 1
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full
pipolicylabelhits	<Double>	Read-only	Number of times policy label was invoked.
pipolicylabelhitsrate	<Double>	Read-only	Rate (/s) counter for pipolicylabelhits

Operations

(click to see Properties)

- GET (ALL)
- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/cmppolicylabel **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/cmppolicylabel? **args=labelname: <String_value> ,detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get cmppolicylabel resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/cmppolicylabel? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "cmppolicylabel": [ {

"labelname":<String_value>,

"pipolicylabelhits":<Double_value>,

"pipolicylabelhitsrate":<Double_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/stat/cmppolicylabel/ labelname_value><String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "cmppolicylabel": [ {

"labelname":<String_value>,

"pipolicylabelhits":<Double_value>,

"pipolicylabelhitsrate":<Double_value>

}]}
```

contentinspection

CI

Content Inspection

NAME	DESCRIPTION
contentinspection	Statistics for contentinspection.
contentinspectionpolicy	Statistics for ContentInspection policy resource.
contentinspectionpolicylabel	Statistics for ContentInspection policy label resource.

contentinspection

Statistics for contentinspection.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
clearstats	<String>	Read-write	Clear the statsistics / counters.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = basic, full
inlinerequestssent	<Double>	Read-only	HTTP/HTTPS requests sent for ContentInspection.
inlineresponsessent	<Double>	Read-only	HTTP/HTTPS responses sent for ContentInspection.
inlinereqbytessent	<Double>	Read-only	Number of bytes transfered for requests to IPS
inlinereqbytesrecv	<Double>	Read-only	Number of bytes received for requests from IPS
inlinerespbytessent	<Double>	Read-only	Number of bytes transfered for responses to IPS
inlinerespbytesrecv	<Double>	Read-only	Number of bytes received for responses from IPS
inlineserverdownreset	<Double>	Read-only	Number of requests Reset when Inline device is down
inlineserverdowndrop	<Double>	Read-only	Number of requests Dropped when Inline device is down
inlineserverdownbypass	<Double>	Read-only	Number of requests bypass content Inspection Module when Inline device is down

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
inlinegeneratedresponses	<Double>	Read-only	Number of Inline device generated Responses
mirrorrequestssent	<Double>	Read-only	Number of requests sent for Intrusion Detection
mirrorresponsessent	<Double>	Read-only	Number of responses sent for Intrusion Detection
mirrorreqbytessent	<Double>	Read-only	Number of request Bytes sent for Intrusion Detection
mirrorrespbytessent	<Double>	Read-only	Number of response Bytes sent for Intrusion Detection
mirrorserverdownreset	<Double>	Read-only	Number of requests Reset when Mirror device is down
mirrorserverdowndrop	<Double>	Read-only	Number of requests Dropped when Mirror device is down
mirrorserverdownbypass	<Double>	Read-only	Number of requests bypass ContentInspection module when Mirror device is down
icapreqmodrequests	<Double>	Read-only	Number of requests sent to ICAP Server
icaprespmodrequests	<Double>	Read-only	Number of responses sent for Intrusion DEtection

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
icappreviewenabledrequests	<Double>	Read-only	Number of preview requests for ICAP
icap204enabledrequests	<Double>	Read-only	Number of 204 Rquests
icap100contrecv	<Double>	Read-only	Number of 100-continue responses received
icap204nocontentrecv	<Double>	Read-only	Number of 204 No content responses received
icapadaptiverequests	<Double>	Read-only	Number of Adaptive requests
icapadaptiveresponses	<Double>	Read-only	Number of Adaptive Responses
icapcalloutinitiated	<Double>	Read-only	Number of callout Requests started
icapcalloutcompleted	<Double>	Read-only	Number of callout requests finished
icaperrorshandled	<Double>	Read-only	Number of errors sent
icapserverdownreset	<Double>	Read-only	Number of requests for which serverdown Reset Action is taken
icapserverdowndrop	<Double>	Read-only	Number of requests for which serverdown Drop Action is taken
icapserverdownbypass	<Double>	Read-only	Number of requests for which serverdown Bypass Action is taken

Operations

(click to see Properties)

- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/contentinspection **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/contentinspection? **args=detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get contentinspection resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/contentinspection? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "contentinspection": [ {

"inlinerespbytessent":<Double_value>,

"mirrorserverdowndrop":<Double_value>,

"inlinerespbytesrecv":<Double_value>,

"icapadaptiverequests":<Double_value>,

"inlinereqbytesrecv":<Double_value>,

"icaperrorshandled":<Double_value>,

"inlineserverdownreset":<Double_value>,

"icap204nocontentrecv":<Double_value>,

"icapcalloutinitiated":<Double_value>,

"inlineresponsessent":<Double_value>,

"icapadaptiveresponses":<Double_value>,
```

```
"icaprespmodrequests":<Double_value>,

"inlinerequestssent":<Double_value>,

"mirrorreqbytessent":<Double_value>,

"icapserverdowndrop":<Double_value>,

"mirrorserverdownbypass":<Double_value>,

"icapserverdownbypass":<Double_value>,

"icapreqmodrequests":<Double_value>,

"icappreviewenabledrequests":<Double_value>,

"mirrorrespbytessent":<Double_value>,

"inlineserverdowndrop":<Double_value>,

"mirrorserverdownreset":<Double_value>,

"icap100contrecv":<Double_value>,

"icapserverdownreset":<Double_value>,

"icap204enabledrequests":<Double_value>,

"inlinereqbytessent":<Double_value>,

"mirrorrequestssent":<Double_value>,

"inlineserverdownbypass":<Double_value>,

"icapcalloutcompleted":<Double_value>,

"inlinegeneratedresponses":<Double_value>,

"mirrorresponsessent":<Double_value>

}]}
```

contentinspectionpolicy

Statistics for ContentInspection policy resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the contentInspection policy for which to show detailed statistics. Minimum length = 1
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full
pipolicyhits	<Double>	Read-only	Number of hits on the policy
pipolicyhitsrate	<Double>	Read-only	Rate (/s) counter for pipolicyhits
pipolicyundefhits	<Double>	Read-only	Number of undef hits on the policy
pipolicyundefhitsrate	<Double>	Read-only	Rate (/s) counter for pipolicyundefhits

Operations

(click to see Properties)

- GET (ALL)
- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/contentinspectionpolicy **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/contentinspectionpolicy? **args=name: <String_value> ,detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get contentinspectionpolicy resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/contentinspectionpolicy? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "contentinspectionpolicy": [ {

"name":<String_value>,

"pipolicyundefhits":<Double_value>,

"pipolicyhits":<Double_value>,

"pipolicyundefhitsrate":<Double_value>,

"pipolicyhitsrate":<Double_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/stat/contentinspectionpolicy/ name_value><String>
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "contentinspectionpolicy": [ {

"name":<String_value>,

"pipolicyundefhits":<Double_value>,

"pipolicyhits":<Double_value>,

"pipolicyundefhitsrate":<Double_value>,

"pipolicyhitsrate":<Double_value>

}]}
```

contentinspectionpolicylabel

Statistics for ContentInspection policy label resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
labelname	<String>	Read-write	Name of the contentInspection policy label. Minimum length = 1
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full
pipolicylabelhits	<Double>	Read-only	Number of times policy label was invoked.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
pipolicylabelhitsrate	<Double>	Read-only	Rate (/s) counter for pipolicylabelhits

Operations

(click to see Properties)

- GET (ALL)
- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/contentinspectionpolicylabel **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/contentinspectionpolicylabel? **args=labelname: <String_value> ,detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get contentinspectionpolicylabel resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/contentinspectionpolicylabel? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "contentinspectionpolicylabel": [ {

"labelname":<String_value>,

"pipolicylabelhitsrate":<Double_value>,

"pipolicylabelhits":<Double_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/stat/contentinspectionpolicylabel/ labelname_value><String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "contentinspectionpolicylabel": [ {

"labelname":<String_value>,

"pipolicylabelhitsrate":<Double_value>,

"pipolicylabelhits":<Double_value>

}]}
```

cr

Cache Redirection

Cache redirection statistics. The cache redirection feature can transparently redirect cacheable HTTP requests to a cache and send non-cacheable or dynamic HTTP requests to the origin server. A cache stores or caches frequently requested web content and serves such web content to a client on behalf of the origin servers, alleviating the load on the origin server farm.

NAME	DESCRIPTION
crvserver	Statistics for CR virtual server resource.

crvserver

Statistics for CR virtual server resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of a specific cache redirection virtual server. Minimum length = 1
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full
primaryipaddress	<String>	Read-only	The IP address on which the service is running.
primaryport	<Integer>	Read-only	The port on which the service is running.
type	<String>	Read-only	Protocol associated with the vserver
state	<String>	Read-only	Current state of the server. There are seven possible values: UP(7), DOWN(1), UNKNOWN(2), BUSY(3), OFS(Out of Service)(4),

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			TROFS(Transition Out of Service)(5), TROFS_DOWN(Down When going Out of Service)(8)
tothits	<Double>	Read-only	Total vserver hits
hitsrate	<Double>	Read-only	Rate (/s) counter for tothits
totalrequests	<Double>	Read-only	Total number of requests received on this service or virtual server. (This applies to HTTP/SSL services and servers.)
requestsrate	<Double>	Read-only	Rate (/s) counter for totalrequests
totalresponses	<Double>	Read-only	Number of responses received on this service or virtual server. (This applies to HTTP/SSL services and servers.)
responsesrate	<Double>	Read-only	Rate (/s) counter for totalresponses
totalrequestbytes	<Double>	Read-only	Total number of request bytes received on this service or virtual server.
requestbytesrate	<Double>	Read-only	Rate (/s) counter for totalrequestbytes

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
totalresponsebytes	<Double>	Read-only	Number of response bytes received by this service or virtual server.
responsebytesrate	<Double>	Read-only	Rate (/s) counter for totalresponsebytes
totalpktsrecvd	<Double>	Read-only	Total number of packets received by this service or virtual server.
pktsrecvdrate	<Double>	Read-only	Rate (/s) counter for totalpktsrecvd
totalpktssent	<Double>	Read-only	Total number of packets sent.
pktssentrate	<Double>	Read-only	Rate (/s) counter for totalpktssent
invalidrequestresponse	<Double>	Read-only	Number invalid requests/responses on this vserver
invalidrequestresponsedropped	<Double>	Read-only	Number invalid requests/responses dropped on this vserver

Operations

(click to see Properties)

- GET (ALL)
- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/crvserver **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/crvserver? **args=name: <String_value> ,detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get crvserver resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/crvserver? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "crvserver": [ {

"name":<String_value>,

"responsebytesrate":<Double_value>,

"type":<String_value>,

"state":<String_value>,

"primaryipaddress":<String_value>,

"totalresponsebytes":<Double_value>,

"hitsrate":<Double_value>,

"pktsrecvdrate":<Double_value>,

"requestbytesrate":<Double_value>,

"totalresponses":<Double_value>,

"invalidrequestresponsedropped":<Double_value>,

"totalpktsrecvd":<Double_value>,

"responsesrate":<Double_value>,

"totalrequests":<Double_value>,

"tothits":<Double_value>,
```

```
"pktssentrate":<Double_value>,

"invalidrequestresponse":<Double_value>,

"totalrequestbytes":<Double_value>,

"primaryport":<Integer_value>,

"totalpktssent":<Double_value>,

"requestsrate":<Double_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/stat/crvserver/ name_value><String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "crvserver": [ {

"name":<String_value>,

"responsebytesrate":<Double_value>,

"type":<String_value>,
```

```
"state":<String_value>,

"primaryipaddress":<String_value>,

"totalresponsebytes":<Double_value>,

"hitsrate":<Double_value>,

"pktsrecvdrate":<Double_value>,

"requestbytesrate":<Double_value>,

"totalresponses":<Double_value>,

"invalidrequestresponsedropped":<Double_value>,

"totalpktsrecvd":<Double_value>,

"responsesrate":<Double_value>,

"totalrequests":<Double_value>,

"tothits":<Double_value>,

"pktssentrate":<Double_value>,

"invalidrequestresponse":<Double_value>,

"totalrequestbytes":<Double_value>,

"primaryport":<Integer_value>,

"totalpktssent":<Double_value>,

"requestsrate":<Double_value>

}]}
```

cs

Content Switching

Content Switching statistics. Content Switching feature that enables you to direct traffic to servers on the basis of content.

NAME	DESCRIPTION
csvserver	Statistics for CS virtual server resource.

csvserver

Statistics for CS virtual server resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the content switching virtual server for which to display statistics. To display statistics for all configured Content Switching virtual servers, do not specify a value for this parameter. Minimum length = 1
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full
avgcltttlb	<Double>	Read-only	Average TTLB between the client and the server. TTLB is the time interval between sending the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			request packet to a service and receiving the ACK for response from client.
cltresponsetimeapdex	<Double>	Read-only	Vserver APDEX index based on client response times.
establishedconn	<Double>	Read-only	Number of client connections in ESTABLISHED state.
primaryipaddress	<String>	Read-only	The IP address on which the service is running.
primaryport	<Integer>	Read-only	The port on which the service is running.
type	<String>	Read-only	Protocol associated with the vserver
state	<String>	Read-only	Current state of the server. There are seven possible values: UP(7), DOWN(1), UNKNOWN(2), BUSY(3), OFS(Out of Service)(4), TROFS(Transition Out of Service)(5), TROFS_DOWN(Down When going Out of Service)(8)
tothits	<Double>	Read-only	Total vserver hits

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
hitsrate	<Double>	Read-only	Rate (/s) counter for tothits
totalrequests	<Double>	Read-only	Total number of requests received on this service or virtual server. (This applies to HTTP/SSL services and servers.)
requestsrate	<Double>	Read-only	Rate (/s) counter for totalrequests
totalresponses	<Double>	Read-only	Number of responses received on this service or virtual server. (This applies to HTTP/SSL services and servers.)
responsesrate	<Double>	Read-only	Rate (/s) counter for totalresponses
totalrequestbytes	<Double>	Read-only	Total number of request bytes received on this service or virtual server.
requestbytesrate	<Double>	Read-only	Rate (/s) counter for totalrequestbytes
totalresponsebytes	<Double>	Read-only	Number of response bytes received by this service or virtual server.
responsebytesrate	<Double>	Read-only	Rate (/s) counter for totalresponsebytes

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
totalpktsrecvd	<Double>	Read-only	Total number of packets received by this service or virtual server.
pktsrecvdrate	<Double>	Read-only	Rate (/s) counter for totalpktsrecvd
totalpktssent	<Double>	Read-only	Total number of packets sent.
pktssentrate	<Double>	Read-only	Rate (/s) counter for totalpktssent
curclntconnections	<Double>	Read-only	Number of current client connections.
cursrvrconnections	<Double>	Read-only	Number of current connections to the actual servers behind the virtual server.
curpersistencesessions	<Double>	Read-only	current vserver owned persistence sessions
curbackuppersistencesessions	<Double>	Read-only	current vserver owned backup persistence sessions
sothreshold	<Double>	Read-only	Spill Over Threshold set on the VServer.
totspillovers	<Double>	Read-only	Number of times vserver experienced spill over.
labelledconn	<Double>	Read-only	Number of Labeled connection on this vserver

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
pushlabel	<Double>	Read-only	Number of labels for this push vserver.
deferredreq	<Double>	Read-only	Number of deferred request on this vserver
deferredreqrate	<Double>	Read-only	Rate (/s) counter for deferredreq
invalidrequestrespon se	<Double>	Read-only	Number invalid requests/responses on this vserver
invalidrequestrespon sedropped	<Double>	Read-only	Number invalid requests/responses dropped on this vserver
totvserverdownbacku phits	<Double>	Read-only	Number of times traffic was diverted to backup vserver since primary vserver was DOWN.
curmptcpsessions	<Double>	Read-only	Current Multipath TCP sessions
cursubflowconn	<Double>	Read-only	Current Multipath TCP subflows
httpmaxhdrszpkts	<Double>	Read-only	Number of http max header size packet parsing failures
httpmaxhdrfldlenpkts	<Double>	Read-only	Number of HTTP requests exceeding max header field length

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
tcpmaxooopkts	<Double>	Read-only	No of times max out of order packets reached
totclttlbtransactions	<Double>	Read-only	Total transactions where client TTLB is calculated.
toleratingttlbtransactions	<Double>	Read-only	Tolerable transactions based on APDEX threshold (>T ;; <4T).
frustratingttlbtransactions	<Double>	Read-only	Frustrating transactions based on APDEX threshold (>4T).

Operations

(click to see Properties)

- GET (ALL)
- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.
- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/csvserver **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/csvserver? **args=name: <String_value> ,detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get csvserver resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/csvserver? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "csvserver": [ {

"name":<String_value>,

"state":<String_value>,

"toleratingttlbtransactions":<Double_value>,

"httpmaxhdrfldlenpkts":<Double_value>,

"deferredreqrate":<Double_value>,

"type":<String_value>,

"responsebytesrate":<Double_value>,

"curclntconnections":<Double_value>,

"totspillovers":<Double_value>,

"labelledconn":<Double_value>,

"totalpktsrecvd":<Double_value>,

"cursubflowconn":<Double_value>,

"curbackuppersistencesessions":<Double_value>,

"tcpmaxooopkts":<Double_value>,

"cursrvrconnections":<Double_value>,

"invalidrequestresponsedropped":<Double_value>,

"totalresponsebytes":<Double_value>,

"pktsrecvdrate":<Double_value>,

"hitsrate":<Double_value>,

"totalresponses":<Double_value>,

"requestbytesrate":<Double_value>,
```

```
"primaryipaddress":<String_value>,

"establishedconn":<Double_value>,

"httpmaxhdrszpkts":<Double_value>,

"totalrequests":<Double_value>,

"responsesrate":<Double_value>,

"curmptcpsessions":<Double_value>,

"avgclttlb":<Double_value>,

"pushlabel":<Double_value>,

"totclttlbtransactions":<Double_value>,

"totalpktssent":<Double_value>,

"cltresponsetimeapdex":<Double_value>,

"totvserverdownbackuphits":<Double_value>,

"deferredreq":<Double_value>,

"requestsrate":<Double_value>,

"primaryport":<Integer_value>,

"curpersistencesessions":<Double_value>,

"invalidrequestresponse":<Double_value>,

"totalrequestbytes":<Double_value>,

"sothreshold":<Double_value>,

"tothits":<Double_value>,

"frustratingttlbtransactions":<Double_value>,

"pktssentrate":<Double_value>
```

```
}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/stat/csvserver/ name_value><String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "csvserver": [ {

"name":<String_value>,

"state":<String_value>,

"toleratingttlbtransactions":<Double_value>,

"httpmaxhdrfldlenpkts":<Double_value>,

"deferredreqrate":<Double_value>,

"type":<String_value>,

"responsebytesrate":<Double_value>,

"curclntconnections":<Double_value>,

"totspillovers":<Double_value>,
```

```
"labelledconn":<Double_value>,

"totalpktsrecvd":<Double_value>,

"cursubflowconn":<Double_value>,

"curbackuppersistencesessions":<Double_value>,

"tcpmaxooopkts":<Double_value>,

"cursrvrconnections":<Double_value>,

"invalidrequestresponsedropped":<Double_value>,

"totalresponsebytes":<Double_value>,

"pktsrecvdrate":<Double_value>,

"hitsrate":<Double_value>,

"totalresponses":<Double_value>,

"requestbytesrate":<Double_value>,

"primaryipaddress":<String_value>,

"establishedconn":<Double_value>,

"httpmaxhdrszpkts":<Double_value>,

"totalrequests":<Double_value>,

"responsesrate":<Double_value>,

"curmptcpsessions":<Double_value>,

"avgclttlb":<Double_value>,

"pushlabel":<Double_value>,

"totclttlbtransactions":<Double_value>,

"totalpktssent":<Double_value>,
```

```
"cltresponsetimeapdex":<Double_value>,

"totvserverdownbackuphits":<Double_value>,

"deferredreq":<Double_value>,

"requestsrate":<Double_value>,

"primaryport":<Integer_value>,

"curpersistencesessions":<Double_value>,

"invalidrequestresponse":<Double_value>,

"totalrequestbytes":<Double_value>,

"sothreshold":<Double_value>,

"tothits":<Double_value>,

"frustratingttlbtransactions":<Double_value>,

"pktssentrate":<Double_value>

}]}
```


dns

Domain Name Service

Domain Name Service(DNS) statistics.

NAME	DESCRIPTION
dns	Statistics for dns.
dnspolicylabel	Statistics for dns policy label resource.
dnsrecords	

dns

Statistics for dns.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full
dnstotqueries	<Double>	Read-only	Total number of DNS queries received.
dnsqueriesrate	<Double>	Read-only	Rate (/s) counter for dnstotqueries
dnstotmultiquery	<Double>	Read-only	Total number of Multi Query request received.
dnstotanswers	<Double>	Read-only	Total number of DNS responses received.
dnsanswersrate	<Double>	Read-only	Rate (/s) counter for dnstotanswers
dnstotserverresponse	<Double>	Read-only	Total number of Server responses received.
dnsserverresponserate	<Double>	Read-only	Rate (/s) counter for dnstotserverresponse
dnstotrecupdate	<Double>	Read-only	Total number of record updates.
dnscurcachesize	<Double>	Read-only	Current DNS cache size

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
dnscurnegcachesize	<Double>	Read-only	Current Negative DNS cache size
dnstotjumboqueries	<Double>	Read-only	Total number of Jumbo DNS queries received over UDP.
dnsjumboqueriesrate	<Double>	Read-only	Rate (/s) counter for dnstotjumboqueries
dnstotjumboanswers	<Double>	Read-only	Total number of Jumbo DNS responses sent over UDP.
dnsjumboanswersrate	<Double>	Read-only	Rate (/s) counter for dnstotjumboanswers
dnstotjumboserverresponses	<Double>	Read-only	Total number of Jumbo DNS responses received over UDP.
dnsjumboserverresponsesrate	<Double>	Read-only	Rate (/s) counter for dnstotjumboserverresponses
dnstotauthans	<Double>	Read-only	Number of queries which were authoritatively answered.
dnstotserverquery	<Double>	Read-only	Total number of Server queries sent.
dnsserverqueryrate	<Double>	Read-only	Rate (/s) counter for dnstotserverquery
dnstotcacheflush	<Double>	Read-only	Total number of times cache was flushed.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
dnstotcacheentriesflush	<Double>	Read-only	Total number of cache entries flushed.
dnscurnoauthentries	<Double>	Read-only	Total number of non-authoritative entries.
dnscurauthentries	<Double>	Read-only	Total number of authoritative entries.
dnstotauthnonames	<Double>	Read-only	Number of queries for which no record was found.
dnstotunsupportedresponseclass	<Double>	Read-only	Total number of responses for which response types were unsupported.
dnstotinvalidqueryformat	<Double>	Read-only	Total number of queries whose format was invalid.
dnstotstrayanswer	<Double>	Read-only	Total number of stray answers.
dnstotresponsebadlen	<Double>	Read-only	Number of DNS responses received with invalid resoure data length.
dnstotreqrefusals	<Double>	Read-only	Number of DNS requests refused.
dnserrnullattack	<Double>	Read-only	Total number of queries received where all the counts are 0.
dnstotunsupportedresponsetype	<Double>	Read-only	Total number of responses for which response type

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			requested was unsupported.
dnstotunsupportedqueryclass	<Double>	Read-only	Total number of queries for which query class was unsupported.
dnstotnonauthnodatas	<Double>	Read-only	Total number of responses for which there was a format error.
dnstotnodataresps	<Double>	Read-only	Number of DNS responses received without answer.
dnstotmultiquerydisableerror	<Double>	Read-only	Total number of times a multi query was disabled and received a multi query.
dnstotothererrors	<Double>	Read-only	Total number of other errors.
dns64totqueries	<Double>	Read-only	Total number of DNS64 queries recieved.
dns64queriesrate	<Double>	Read-only	Rate (/s) counter for dns64totqueries
dns64totanswers	<Double>	Read-only	Total number of DNS64 answers served.
dns64answersrate	<Double>	Read-only	Rate (/s) counter for dns64totanswers
dns64totrwanswers	<Double>	Read-only	Total number of DNS64 answers

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			served after rewriting the response.
dns64rwanswersrate	<Double>	Read-only	Rate (/s) counter for dns64totrwanswers
dns64totresponses	<Double>	Read-only	Total number of responses recieved from backend in DNS64 context.
dns64responsesrate	<Double>	Read-only	Rate (/s) counter for dns64totresponses
dns64totgslbqueries	<Double>	Read-only	Total number of DNS64 queries for GSLB domain
dns64gslbqueriesrate	<Double>	Read-only	Rate (/s) counter for dns64totgslbqueries
dns64totgslbanswers	<Double>	Read-only	Total number of DNS64 queries served.
dns64gslbanswersrate	<Double>	Read-only	Rate (/s) counter for dns64totgslbanswers
dns64tottcanswers	<Double>	Read-only	Total number of Answers served with TC bit set in DNS64 context.
dns64tcanswersrate	<Double>	Read-only	Rate (/s) counter for dns64tottcanswers
dns64totsvraqueries	<Double>	Read-only	Total number of Queries sent by DNS64 module to backend.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
dns64svraqueriesrate	<Double>	Read-only	Rate (/s) counter for dns64totsvraqueries
dns64totaaaabypass	<Double>	Read-only	Total number of times AAAA query has been bypassed in DNS64 trnsaction.
dns64aaaabypassrate	<Double>	Read-only	Rate (/s) counter for dns64totaaaabypass
dns64tottcpqueries	<Double>	Read-only	Total number of dns64 queries over TCP
dns64tcpqueriesrate	<Double>	Read-only	Rate (/s) counter for dns64tottcpqueries
dns64activepolicies	<Double>	Read-only	Total number of active dns64 policies
dns64totnodataresp	<Double>	Read-only	Total number of responses recieved from backend with ancount 0
dns64nodataresprate	<Double>	Read-only	Rate (/s) counter for dns64totnodataresp
dnstotnsrecqueries	<Double>	Read-only	Total number of NS queries received.
dnsnsrecqueriesrate	<Double>	Read-only	Rate (/s) counter for dnstotnsrecqueries
dnstotsoarecqueries	<Double>	Read-only	Total number of SOA queries received.
dnssoarecqueriesrate	<Double>	Read-only	Rate (/s) counter for dnstotsoarecqueries

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
dnstotptrrecqueries	<Double>	Read-only	Total number of PTR queries received.
dnsptrrecqueriesrate	<Double>	Read-only	Rate (/s) counter for dnstotptrrecqueries
dnstotsrvrecqueries	<Double>	Read-only	Total number of SRV queries received.
dnssrvrecqueriesrate	<Double>	Read-only	Rate (/s) counter for dnstotsrvrecqueries
dnstotaresponse	<Double>	Read-only	Total number of A responses received.
dnsaresponserate	<Double>	Read-only	Rate (/s) counter for dnstotaresponse
dnstotcnameresponse	<Double>	Read-only	Total number of CNAME responses received.
dnscnameresponserate	<Double>	Read-only	Rate (/s) counter for dnstotcnameresponse
dnstotmxresponse	<Double>	Read-only	Total number of MX responses received.
dnsmxresponserate	<Double>	Read-only	Rate (/s) counter for dnstotmxresponse
dnstotanyresponse	<Double>	Read-only	Total number of ANY responses received.
dnsanyresponserate	<Double>	Read-only	Rate (/s) counter for dnstotanyresponse
dnstotnsrecupdate	<Double>	Read-only	Total number of NS record updates.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
dnstotsoarecupdate	<Double>	Read-only	Total number of SOA record updates.
dnstotptrrecupdate	<Double>	Read-only	Total number of PTR record updates.
dnstotsrvrecupdate	<Double>	Read-only	Total number of SRV record updates.
dnstotaaaarecqueries	<Double>	Read-only	Total number of AAAA queries received.
dnsaaaarecqueriesrate	<Double>	Read-only	Rate (/s) counter for dnstotaaaarecqueries
dnstotarecqueries	<Double>	Read-only	Total number of A queries received.
dnsarecqueriesrate	<Double>	Read-only	Rate (/s) counter for dnstotarecqueries
dnstotcnamerecqueries	<Double>	Read-only	Total number of CNAME queries received.
dnscnamerecqueriesrate	<Double>	Read-only	Rate (/s) counter for dnstotcnamerecqueries
dnstotmxrecqueries	<Double>	Read-only	Total number of MX queries received.
dnsmxrecqueriesrate	<Double>	Read-only	Rate (/s) counter for dnstotmxrecqueries
dnstotanyqueries	<Double>	Read-only	Total number of ANY queries received.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
dnsanyqueriesrate	<Double>	Read-only	Rate (/s) counter for dnstotanyqueries
dnstotaaaaresponse	<Double>	Read-only	Total number of AAAA responses received.
dnsaaaaresponserate	<Double>	Read-only	Rate (/s) counter for dnstotaaaaresponse
dnstotnsresponse	<Double>	Read-only	Total number of NS responses received.
dnsnsresponserate	<Double>	Read-only	Rate (/s) counter for dnstotnsresponse
dnstotsoaresponse	<Double>	Read-only	Total number of SOA responses received.
dnssoaresponserate	<Double>	Read-only	Rate (/s) counter for dnstotsoaresponse
dnstotptrresponse	<Double>	Read-only	Total number of PTR responses received.
dnsptrresponserate	<Double>	Read-only	Rate (/s) counter for dnstotptrresponse
dnstotsrvresponse	<Double>	Read-only	Total number of SRV responses received.
dnssrvresponserate	<Double>	Read-only	Rate (/s) counter for dnstotsrvresponse
dnstotaaaarecupdate	<Double>	Read-only	Total number of AAAA record updates.
dnstotarecupdate	<Double>	Read-only	Total number of A record updates.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
dnstotmxrecupdate	<Double>	Read-only	Total number of MX record updates.
dnstotcnamerecupdate	<Double>	Read-only	Total number of CNAME record updates.
dnscuraaaarecord	<Double>	Read-only	Total number of AAAA records.
dnscurarecord	<Double>	Read-only	Total number of A records.
dnscurmxrecord	<Double>	Read-only	Total number of MX records.
dnscurcnamerecord	<Double>	Read-only	Total number of CNAME records.
dnscurnsrecord	<Double>	Read-only	Total number of NS records.
dnscursoarecord	<Double>	Read-only	Total number of SOA records.
dnscurptrrecord	<Double>	Read-only	Total number of PTR records.
dnscursrvrecord	<Double>	Read-only	Total number of SRV records.
dnstotaaaarecfailed	<Double>	Read-only	Total number of times AAAA record lookup failed.
dnstotarecfailed	<Double>	Read-only	Total number of times A record lookup failed.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
dnstotmxrecfailed	<Double>	Read-only	Total number of times MX record lookup failed.
dnstotptrrecfailed	<Double>	Read-only	Total number of times PTR record lookup failed.
dnstotnsrecfailed	<Double>	Read-only	Total number of times NS record lookup failed.
dnstotcnamerecfailed	<Double>	Read-only	Total number of times CNAME record lookup failed.
dnstotsoarecfailed	<Double>	Read-only	Total number of times SOA record lookup failed.
dnstotsrvrecfailed	<Double>	Read-only	Total number of times SRV record lookup failed.
dnstotanyrecfailed	<Double>	Read-only	Total number of times ANY query lookup failed.
dnstotunsupportedqueries	<Double>	Read-only	Total number of requests for which query type requested was unsupported.

Operations

(click to see Properties)

- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/dns **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/dns? **args=detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get dns resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/dns? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "dns": [ {

"dnstotnodataresps":<Double_value>,

"dnscurmxrecord":<Double_value>,

"dnstotanyrecfailed":<Double_value>,

"dnssoaresponserate":<Double_value>,

"dnsptrresponserate":<Double_value>,

"dnstotmultiquery":<Double_value>,

"dnscnameresponserate":<Double_value>,

"dnscnamerecqueriesrate":<Double_value>,

"dnsnsresponserate":<Double_value>,

"dns64tcpqueriesrate":<Double_value>,

"dnstotmxresponse":<Double_value>,

"dnstotsoaresponse":<Double_value>,

"dnsserverresponserate":<Double_value>,

"dns64totaaaabypass":<Double_value>,

"dns64responsesrate":<Double_value>,
```

```
"dnsnsrecqueriesrate":<Double_value>,

"dns64gslbqueriesrate":<Double_value>,

"dnstotsoarecqueries":<Double_value>,

"dns64tottcanswers":<Double_value>,

"dnstotsrvrecupdate":<Double_value>,

"dns64totresponses":<Double_value>,

"dnsptrrecqueriesrate":<Double_value>,

"dnssoarecqueriesrate":<Double_value>,

"dns64svraqueriesrate":<Double_value>,

"dns64totnodataresp":<Double_value>,

"dns64totgslbanswers":<Double_value>,

"dnsaaaarecqueriesrate":<Double_value>,

"dnstotaaaarecqueries":<Double_value>,

"dnstotptrrecfailed":<Double_value>,

"dnstotmultiquerydisableerror":<Double_value>,

"dnstotunsupportedqueryclass":<Double_value>,

"dnstotcacheentriesflush":<Double_value>,

"dnstotanyqueries":<Double_value>,

"dnsaaaaresponserate":<Double_value>,

"dnstotptrresponse":<Double_value>,

"dnscursrvrecord":<Double_value>,

"dns64tcanswersrate":<Double_value>,
```

```
"dns64rwanswersrate":<Double_value>,

"dns64aaaabypassrate":<Double_value>,

"dns64answersrate":<Double_value>,

"dnstotnsrecfailed":<Double_value>,

"dnstotmxrecupdate":<Double_value>,

"dnstotptrrecqueries":<Double_value>,

"dnscurauthentries":<Double_value>,

"dns64queriesrate":<Double_value>,

"dnstotnsrecqueries":<Double_value>,

"dnscurnegcachesize":<Double_value>,

"dnstotunsupportedresponseclass":<Double_value>,

"dns64activepolicies":<Double_value>,

"dnstotresponsebadlen":<Double_value>,

"dnstotjumboserverresponses":<Double_value>,

"dnstotserverresponse":<Double_value>,

"dnsjumboserverresponsesrate":<Double_value>,

"dnscurcachesize":<Double_value>,

"dnstotcacheflush":<Double_value>,

"dnstotarecqueries":<Double_value>,

"dnstotserverquery":<Double_value>,

"dnscurarecord":<Double_value>,

"dnstotinvalidqueryformat":<Double_value>,
```

```
"dnstotanyresponse":<Double_value>,

"dnstotunsupportedqueries":<Double_value>,

"dnstotarecfailed":<Double_value>,

"dnstotsoarecfailed":<Double_value>,

"dnserrnullattack":<Double_value>,

"dnstotmxrecfailed":<Double_value>,

"dnstotnsrecupdate":<Double_value>,

"dnsqueriesrate":<Double_value>,

"dnstotauthnonames":<Double_value>,

"dnstotjumboqueries":<Double_value>,

"dnsmxrecqueriesrate":<Double_value>,

"dnstotmxrecqueries":<Double_value>,

"dnscuraaaarecord":<Double_value>,

"dnstotsrvrecqueries":<Double_value>,

"dnstotrecupdate":<Double_value>,

"dnstotcnamerecqueries":<Double_value>,

"dns64tottcpqueries":<Double_value>,

"dns64totgslbqueries":<Double_value>,

"dns64gslbanswersrate":<Double_value>,

"dnscurnoauthentries":<Double_value>,

"dnsmxresponserate":<Double_value>,

"dnscurptrrecord":<Double_value>,
```

```
"dnstotsrvresponse":<Double_value>,

"dnstotqueries":<Double_value>,

"dnscurcnamerecord":<Double_value>,

"dnsarecqueriesrate":<Double_value>,

"dnstotjumboanswers":<Double_value>,

"dnsjumboanswersrate":<Double_value>,

"dnsanyqueriesrate":<Double_value>,

"dns64totanswers":<Double_value>,

"dns64nodatarespsrate":<Double_value>,

"dnstotsoarecupdate":<Double_value>,

"dnsanyresponserate":<Double_value>,

"dnsanswersrate":<Double_value>,

"dnstotarecupdate":<Double_value>,

"dnstotreqrefusals":<Double_value>,

"dnstotstrayanswer":<Double_value>,

"dnstotaaaaresponse":<Double_value>,

"dnstotnonauthnodatas":<Double_value>,

"dnscursoarecord":<Double_value>,

"dnscurnsrecord":<Double_value>,

"dnstotcnameresponse":<Double_value>,

"dnssrvresponserate":<Double_value>,

"dnstotanswers":<Double_value>,
```

```
"dnsjumboqueriesrate":<Double_value>,

"dnstotaaaarecfailed":<Double_value>,

"dns64totqueries":<Double_value>,

"dnstotothererrors":<Double_value>,

"dnstotnsresponse":<Double_value>,

"dnstotcnamerecupdate":<Double_value>,

"dnstotauthans":<Double_value>,

"dnsserverqueryrate":<Double_value>,

"dnstotcnamerecfailed":<Double_value>,

"dns64totsvraqueries":<Double_value>,

"dnstotunsupportedresponsetype":<Double_value>,

"dnstotsrvrecfailed":<Double_value>,

"dnstotaresponse":<Double_value>,

"dnsaresponserate":<Double_value>,

"dns64totrwanswers":<Double_value>,

"dnstotaaaarecupdate":<Double_value>,

"dnssrvrecqueriesrate":<Double_value>,

"dnstotptrrecupdate":<Double_value>

}]}
```


dnspolicylabel

Statistics for dns policy label resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
labelname	<String>	Read-write	The name of the dns policy label for which statistics will be displayed. If not given statistics are shown for all dns policylabels. Minimum length = 1
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full
pipolicylabelhits	<Double>	Read-only	Number of times policy label was invoked.
pipolicylabelhitsrate	<Double>	Read-only	Rate (/s) counter for pipolicylabelhits

Operations

(click to see Properties)

- GET (ALL)
- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/dnspolicylabel **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/dnspolicylabel? **args=labelname: <String_value> ,detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get dnspolicylabel resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/dnspolicylabel? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "dnspolicylabel": [ {

"labelname":<String_value>,

"pipolicylabelhits":<Double_value>,

"pipolicylabelhitsrate":<Double_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/stat/dnspolicylabel/ labelname_value><String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "dnspolicylabel": [ {

"labelname":<String_value>,

"pipolicylabelhits":<Double_value>,

"pipolicylabelhitsrate":<Double_value>
```

```
}]}
```

dnsrecords

Read/write properties

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
dnsrecordtype	<String>	Read-write	Display statistics for the specified DNS record or query type or, if a record or query type is not specified, statistics for all record types supported on the Citrix ADC.
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full
dnstotentries	<Double>	Read-only	Total number of DNS record entries
dnstotupdates	<Double>	Read-only	Total number of DNS proactive updates
dnstotresponses	<Double>	Read-only	Total number of DNS server responses
dnstotrequests	<Double>	Read-only	Total number of DNS queries recieved
dnscurentries	<Double>	Read-only	Current number of DNS entries

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
dnstotqueryforexpiredrecord	<Double>	Read-only	Total number of times query was received for expired record
dnstoterrlimits	<Double>	Read-only	Total number of times we have recieved dns record with more entries than we support
dnstoterrrespform	<Double>	Read-only	Total number of times we have recieved malformed responses from the backend
dnstoterraliasex	<Double>	Read-only	Total number of times we have recieved non-cname record for a domain for which an alias exists
dnstoterrnodomains	<Double>	Read-only	Total number of cache misses
dnscurrecords	<Double>	Read-only	Current number of DNS Records

Operations

(click to see Properties)

- GET (ALL)
- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/dnsrecords **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/dnsrecords? **args=dnsrecordtype: <String_value> ,detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get dnsrecords resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/dnsrecords? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "dnsrecords": [ {

"dnsrecordtype":<String_value>,

"dnstoterraliasex":<Double_value>,

"dnstotresponses":<Double_value>,

"dnstoterrrespform":<Double_value>,

"dnscurrecords":<Double_value>,

"dnstoterrnodomains":<Double_value>,

"dnscurentries":<Double_value>,

"dnstotrequests":<Double_value>,

"dnstotupdates":<Double_value>,

"dnstotentries":<Double_value>,

"dnstoterrlimits":<Double_value>,

"dnstotqueryforexpiredrecord":<Double_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/stat/dnsrecords/ dnsrecordtype_value><String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "dnsrecords": [ {

"dnsrecordtype":<String_value>,

"dnstoterraliasex":<Double_value>,

"dnstotresponses":<Double_value>,

"dnstoterrrespform":<Double_value>,

"dnscurrecords":<Double_value>,

"dnstoterrnodomains":<Double_value>,

"dnscurentries":<Double_value>,

"dnstotrequests":<Double_value>,

"dnstotupdates":<Double_value>,

"dnstotentries":<Double_value>,

"dnstoterrlimits":<Double_value>,
```

```
"dnstotqueryforexpiredrecord":<Double_value>

}]}
```

feo

Front-end-optimization

Front end optimization statistics. The system's feature to optimize Web content for performance.

NAME	DESCRIPTION
feo	Statistics for feo.

feo

Statistics for feo.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full
optcacheobjects	<Double>	Read-only	Total number of optimized cache objects ready to be served.
optcacheobjectsrate	<Double>	Read-only	Rate (/s) counter for optcacheobjects
origcacheobjects	<Double>	Read-only	Total number of original cache

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			objects ready to be served.
origcacheobjectsrate	<Double>	Read-only	Rate (/s) counter for origcacheobjects
totalimgsdomainsharded	<Double>	Read-only	Total no of images whose domain has been set from shards.
imgsdomainshardedrate	<Double>	Read-only	Rate (/s) counter for totalimgsdomainsharded
totalimgslazyloaded	<Double>	Read-only	Total number of images modified for lazy loading.
imgslazyloadedrate	<Double>	Read-only	Rate (/s) counter for totalimgslazyloaded
toturireplaced	<Double>	Read-only	Total number of URI replaced.
urireplacedrate	<Double>	Read-only	Rate (/s) counter for toturireplaced
totalimgsinlinedincss	<Double>	Read-only	Total number of images inlined in CSS.
imgsinlinedincssrate	<Double>	Read-only	Rate (/s) counter for totalimgsinlinedincss
totalinlinedjs	<Double>	Read-only	Total number of inlined JS files.
inlinedjsrate	<Double>	Read-only	Rate (/s) counter for totalinlinedjs

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
totalinlinedcss	<Double>	Read-only	Total number of inlined CSS files.
inlinedcssrate	<Double>	Read-only	Rate (/s) counter for totalinlinedcss
totalinlinedimgs	<Double>	Read-only	Total number of inlined images in HTML.
inlinedimgsrate	<Double>	Read-only	Rate (/s) counter for totalinlinedimgs
totaldatasavings	<Double>	Read-only	Total data savings in bytes.
datasavingsrate	<Double>	Read-only	Rate (/s) counter for totaldatasavings
htmlcommentsremoved	<Double>	Read-only	The total number of HTML comments removed.
htmlcommentsremovedrate	<Double>	Read-only	Rate (/s) counter for htmlcommentsremoved
totalcacheextended	<Double>	Read-only	The total number of objects cache extended.
cacheextendedrate	<Double>	Read-only	Rate (/s) counter for totalcacheextended
totalcsscombined	<Double>	Read-only	The total number of CSS combined.
csscombinedrate	<Double>	Read-only	Rate (/s) counter for totalcsscombined

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
totalimporttolink	<Double>	Read-only	The total number of CSS imports converted to links
importtolinkrate	<Double>	Read-only	Rate (/s) counter for totalimporttolink
totaljsmoved	<Double>	Read-only	The total number of JS moved to end.
jsmovedrate	<Double>	Read-only	Rate (/s) counter for totaljsmoved
totalcssmoved	<Double>	Read-only	The total number of CSS moved to head.
cssmovedrate	<Double>	Read-only	Rate (/s) counter for totalcssmoved
totaljsmin	<Double>	Read-only	The total number of JS files minified.
jsminrate	<Double>	Read-only	Rate (/s) counter for totaljsmin
totalcssmin	<Double>	Read-only	The total number of CSS files minified.
cssminrate	<Double>	Read-only	Rate (/s) counter for totalcssmin
totalimgstojxr	<Double>	Read-only	The total number of images converted to JPEGXR format.
imgstojxrrate	<Double>	Read-only	Rate (/s) counter for totalimgstojxr
totalimgstowebp	<Double>	Read-only	The total number of images converted to WEBP format.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
imgstowebprate	<Double>	Read-only	Rate (/s) counter for totalimgstowebp
totaljpegsoptimized	<Double>	Read-only	The total number of JPEG format images optimized.
jpegsoptimizedrate	<Double>	Read-only	Rate (/s) counter for totaljpegsoptimized
totalgifstopng	<Double>	Read-only	The total number of images converted from GIF to PNG format.
gifstopngrate	<Double>	Read-only	Rate (/s) counter for totalgifstopng
totalimgsresized	<Double>	Read-only	The total number of images resized to dimensions in the <img> tag.
imgsresizedrate	<Double>	Read-only	Rate (/s) counter for totalimgsresized

Operations

(click to see Properties)

- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/feo **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/feo? **args=detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get feo resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/feo? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "feo": [ {

"optcacheobjects":<Double_value>,

"datasavingsrate":<Double_value>,

"toturireplaced":<Double_value>,

"imgstowebprate":<Double_value>,

"imgsinlinedincssrate":<Double_value>,

"totalcsscombined":<Double_value>,

"totalimgsdomainsharded":<Double_value>,

"totalimgstojxr":<Double_value>,

"jsminrate":<Double_value>,

"cssminrate":<Double_value>,

"imgslazyloadedrate":<Double_value>,

"totalcssmoved":<Double_value>,

"htmlcommentsremoved":<Double_value>,

"totaljsmin":<Double_value>,

"jpegsoptimizedrate":<Double_value>,

"imgsresizedrate":<Double_value>,

"inlinedimgsrate":<Double_value>,

"cssmovedrate":<Double_value>,

"totalimgstowebp":<Double_value>,
```

```
"totaljsmoved":<Double_value>,

"urireplacedrate":<Double_value>,

"totalimporttolink":<Double_value>,

"cacheextendedrate":<Double_value>,

"csscombinedrate":<Double_value>,

"htmlcommentsremovedrate":<Double_value>,

"totalcacheextended":<Double_value>,

"importtolinkrate":<Double_value>,

"imgstojxrrate":<Double_value>,

"totalinlinedcss":<Double_value>,

"imgsdomainshardedrate":<Double_value>,

"totalcssmin":<Double_value>,

"totaljpegsoptimized":<Double_value>,

"optcacheobjectsrate":<Double_value>,

"gifstopngrate":<Double_value>,

"origcacheobjectsrate":<Double_value>,

"totalinlinedjs":<Double_value>,

"totalimgsinlinedincss":<Double_value>,

"origcacheobjects":<Double_value>,

"totalimgslazyloaded":<Double_value>,

"totalinlinedimgs":<Double_value>,

"inlinedjsrate":<Double_value>,
```

```
"jsmovedrate":<Double_value>,

"inlinedcssrate":<Double_value>,

"totalimgsresized":<Double_value>,

"totalgifstopng":<Double_value>,

"totaldatasavings":<Double_value>

}]}
```

gslb

Global Server Load Balancing

Global Server Load Balancing (GSLB) statistics. GSLB feature ensures that client requests are directed to a best performing site available in a global enterprise and distributed Internet environment.

NAME	DESCRIPTION
gslbdomain	Statistics for GSLB domain resource.
gslbservice	Statistics for GSLB service resource.
gslbservicegroup	Statistics for GSLB service group resource.
gslbservicegroupmember	Statistics for GSLB service group entity resource.
gslbsite	Statistics for GSLB site resource.
gslbvserver	Statistics for Global Server Load Balancing Virtual Server resource.

gslbdomain

Statistics for GSLB domain resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the GSLB domain for which to display statistics. If you do not specify a name, statistics are shown for all configured GSLB domains. Minimum length = 1
dnsrecordtype	<String>	Read-write	. Possible values = A, AAAA, CNAME, NAPTR
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full
dnstotalqueries	<Double>	Read-only	Total number of DNS queries received.
dnsqueriesrate	<Double>	Read-only	Rate (/s) counter for dnstotalqueries
gslbdnsrectype	<String>	Read-only	Type of DNS record returned

Operations

(click to see Properties)

- GET (ALL)
- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/gslbdomain **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/gslbdomain? **args=name: <String_value> ,dnsrecordtype: <String_value> ,dnsrecordtype: <String_value> ,detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get gslbdomain resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/gslbdomain? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "gslbdomain": [ {

"name":<String_value>,

"dnstotalqueries":<Double_value>,

"gslbdnsrectype":<String_value>,

"dnsqueriesrate":<Double_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/stat/gslbdomain/ name_value><String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "gslbdomain": [ {

"name":<String_value>,

"dnstotalqueries":<Double_value>,

"gslbdnsrectype":<String_value>,

"dnsqueriesrate":<Double_value>

}]}
```

gslbservice

Statistics for GSLB service resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
servicename	<String>	Read-write	Name of the GSLB service. Minimum length = 1
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
establishedconn	<Double>	Read-only	Number of client connections in ESTABLISHED state.
primaryipaddress	<String>	Read-only	The IP address on which the service is running.
primaryport	<Integer>	Read-only	The port on which the service is running.
servicetype	<String>	Read-only	The service type of this service.Possible values are ADNS, DNS, MYSQL, RTSP, SSL_DIAMETER, ADNS_TCP, DNS_TCP, NNTP, SIP_UDP, SSL_TCP, ANY, FTP, RADIUS, SNMP, TCP, DHCPRA, HTTP, RDP, SSL, TFTP, DIAMETER, MSSQL, RPCSVR, SSL_BRIDGE, UDP
state	<String>	Read-only	Current state of the server. There are seven possible values: UP(7), DOWN(1), UNKNOWN(2), BUSY(3), OFS(Out of Service)(4), TROFS(Transition Out of Service)(5), TROFS_DOWN(Dow

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			n When going Out of Service)(8)
totalrequestbytes	<Double>	Read-only	Total number of request bytes received on this service or virtual server.
requestbytesrate	<Double>	Read-only	Rate (/s) counter for totalrequestbytes
totalresponsebytes	<Double>	Read-only	Number of response bytes received by this service or virtual server.
responsebytesrate	<Double>	Read-only	Rate (/s) counter for totalresponsebytes
curload	<Double>	Read-only	Load on the service that is calculated from the bound load based monitor.
totalrequests	<Double>	Read-only	Total number of requests received on this service or virtual server. (This applies to HTTP/SSL services and servers.)
requestsrate	<Double>	Read-only	Rate (/s) counter for totalrequests
totalresponses	<Double>	Read-only	Number of responses received on this service or virtual server. (This applies to HTTP/SSL

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			services and servers.)
responsesrate	<Double>	Read-only	Rate (/s) counter for totalresponses
curclntconnections	<Double>	Read-only	Number of current client connections.
cursrvrconnections	<Double>	Read-only	Number of current connections to the actual servers behind the virtual server.
vsvrservicehits	<Double>	Read-only	Number of times that the service has been provided.
vsvrservicehitsrate	<Double>	Read-only	Rate (/s) counter for vsvrservicehits
serviceorder	<Double>	Read-only	Order with which service is bound to vserver

Operations

(click to see Properties)

- GET (ALL)
- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/gslbservice **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/gslbservice? **args=servicename: <String_value> ,detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get gslbservice resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/gslbservice? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "gslbservice": [ {

"servicename":<String_value>,

"totalresponses":<Double_value>,

"requestbytesrate":<Double_value>,

"totalresponsebytes":<Double_value>,

"primaryipaddress":<String_value>,

"establishedconn":<Double_value>,

"cursrvrconnections":<Double_value>,

"vsvrservicehitsrate":<Double_value>,

"servicetype":<String_value>,

"curclntconnections":<Double_value>,

"responsebytesrate":<Double_value>,

"state":<String_value>,

"totalrequestbytes":<Double_value>,

"requestsrate":<Double_value>,

"curload":<Double_value>,

"serviceorder":<Double_value>,
```

```
"primaryport":<Integer_value>,

"totalrequests":<Double_value>,

"responsesrate":<Double_value>,

"vsvrservicehits":<Double_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/stat/gslbservice/ servicename_value><String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "gslbservice": [ {

"servicename":<String_value>,

"totalresponses":<Double_value>,

"requestbytesrate":<Double_value>,

"totalresponsebytes":<Double_value>,

"primaryipaddress":<String_value>,
```

```
"establishedconn":<Double_value>,

"cursrvrconnections":<Double_value>,

"vsvrservicehitsrate":<Double_value>,

"servicetype":<String_value>,

"curclntconnections":<Double_value>,

"responsebytesrate":<Double_value>,

"state":<String_value>,

"totalrequestbytes":<Double_value>,

"requestsrate":<Double_value>,

"curload":<Double_value>,

"serviceorder":<Double_value>,

"primaryport":<Integer_value>,

"totalrequests":<Double_value>,

"responsesrate":<Double_value>,

"vsvrservicehits":<Double_value>

}]}
```

gslbservicegroup

Statistics for GSLB service group resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
servicegroupname	<String>	Read-write	Name of the GSLB service group for which to display settings. Minimum length = 1
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full
state	<String>	Read-only	Current state of the server. There are seven possible values: UP(7), DOWN(1), UNKNOWN(2), BUSY(3), OFS(Out of Service)(4), TROFS(Transition Out of Service)(5), TROFS_DOWN(Down When going Out of Service)(8)
servicetype	<String>	Read-only	The service type of this service.Possible values are ADNS, DNS, MYSQL, RTSP, SSL_DIAMETER, ADNS_TCP, DNS_TCP, NNTP, SIP_UDP, SSL_TCP, ANY, FTP, RADIUS, SNMP, TCP, DHCPRA, HTTP, RDP, SSL, TFTP, DIAMETER,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			MSSQL, RPCSVR, SSL_BRIDGE, UDP

Operations

(click to see Properties)

- GET (ALL)
- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.
- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/gslbservicegroup **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/gslbservicegroup? **args=servicegroupname:**

<String_value> ,detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>

Use this query-parameter to get gslbservicegroup resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/gslbservicegroup? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "gslbservicegroup": [ {

"servicegroupname":<String_value>,

"state":<String_value>,

"servicetype":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/stat/gslbservicegroup/ servicegroupname_value><String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "gslbservicegroup": [ {

"servicegroupname":<String_value>,

"state":<String_value>,

"servicetype":<String_value>

}]}
```

gslbservicegroupmember

Statistics for GSLB service group entity resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
servicegroupname	<String>	Read-write	Displays statistics for the specified GSLB service group.Name of the GSLB service group. Must begin with an ASCII alphanumeric or

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at sign (@), equal sign (=), and hyphen (-) characters.CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my servicegroup" or 'my servicegroup'). Minimum length = 1
ip	<String>	Read-write	IP address of the GSLB service group. Mutually exclusive with the server name parameter.
servername	<String>	Read-write	Name of the server. Mutually exclusive with the IP address parameter. Minimum length = 1
port	<Integer>	Read-write	Port number of the service group member. Range 1 - 65535 * in CLI is represented as

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			65535 in NITRO API
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full
establishedconn	<Double>	Read-only	Number of client connections in ESTABLISHED state.
primaryipaddress	<String>	Read-only	The IP address on which the service is running.
primaryport	<Integer>	Read-only	The port on which the service is running.
servicetype	<String>	Read-only	The service type of this service.Possible values are ADNS, DNS, MYSQL, RTSP, SSL_DIAMETER, ADNS_TCP, DNS_TCP, NNTP, SIP_UDP, SSL_TCP, ANY, FTP, RADIUS, SNMP, TCP, DHCPRA, HTTP, RDP, SSL, TFTP, DIAMETER, MSSQL, RPCSVR, SSL_BRIDGE, UDP
state	<String>	Read-only	Current state of the server. There are seven possible

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			values: UP(7), DOWN(1), UNKNOWN(2), BUSY(3), OFS(Out of Service)(4), TROFS(Transition Out of Service)(5), TROFS_DOWN(Down When going Out of Service)(8)
svcgrpmemberbindingorder	<Double>	Read-only	Order with which service group member is bound to service group
totalrequestbytes	<Double>	Read-only	Total number of request bytes received on this service or virtual server.
requestbytesrate	<Double>	Read-only	Rate (/s) counter for totalrequestbytes
totalresponsebytes	<Double>	Read-only	Number of response bytes received by this service or virtual server.
responsebytesrate	<Double>	Read-only	Rate (/s) counter for totalresponsebytes
curload	<Double>	Read-only	Load on the service that is calculated from the bound load based monitor.
totalrequests	<Double>	Read-only	Total number of requests received on this service or virtual server. (This applies

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			to HTTP/SSL services and servers.)
requestsrate	<Double>	Read-only	Rate (/s) counter for totalrequests
totalresponses	<Double>	Read-only	Number of responses received on this service or virtual server. (This applies to HTTP/SSL services and servers.)
responsesrate	<Double>	Read-only	Rate (/s) counter for totalresponses
curclntconnections	<Double>	Read-only	Number of current client connections.
cursrvrconnections	<Double>	Read-only	Number of current connections to the actual servers behind the virtual server.
serviceorder	<Double>	Read-only	Order with which service is bound to vserver

Operations

(click to see Properties)

- GET (ALL)
- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/gslbservicegroupmember **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/gslbservicegroupmember? **args= servicegroupname:<String_value>, ip: <String_value> ,servername: <String_value> , port:<Integer_value>, detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get gslbservicegroupmember resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/gslbservicegroupmember? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "gslbservicegroupmember": [ {

"servicegroupname":<String_value>,

"state":<String_value>,

"servicetype":<String_value>,

"responsebytesrate":<Double_value>,

"curclntconnections":<Double_value>,

"cursrvrconnections":<Double_value>,

"svcgrpmemberbindingorder":<Double_value>,

"establishedconn":<Double_value>,

"primaryipaddress":<String_value>,

"requestbytesrate":<Double_value>,

"totalresponses":<Double_value>,

"totalresponsebytes":<Double_value>,

"responsesrate":<Double_value>,
```

```
"totalrequests":<Double_value>,

"curload":<Double_value>,

"primaryport":<Integer_value>,

"serviceorder":<Double_value>,

"requestsrate":<Double_value>,

"totalrequestbytes":<Double_value>

}]}
```

gslbsite

Statistics for GSLB site resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
sitename	<String>	Read-write	Name of the GSLB site for which to display detailed statistics. If a name is not specified, basic information about all GSLB sites is displayed. Minimum length = 1
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
sitepublicip	<String>	Read-only	The public IP address of this GSLB site.
siteip	<String>	Read-only	The private IP address of this GSLB site.
sitemepstatus	<String>	Read-only	Indicates the status of the Metric Exchange Policy at this GSLB site.
persexchange	<String>	Read-only	Indicates whether Persistence entries exchange is enabled or disabled at this GSLB site.
nwmetricexchange	<String>	Read-only	Indicates whether network metric exchange is enabled or disabled at this GSLB site.
sitemetricexchange	<String>	Read-only	Indicates whether metric exchange is enabled or disabled at this GSLB site.
sitetype	<String>	Read-only	Indicates whether this GSLB site is local or remote.
siteipstr	<String>	Read-only	The private IP address of this GSLB site.
sitepublicipstr	<String>	Read-only	The public IP address of this GSLB site.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
sitemetricmepstatus	<String>	Read-only	Indicates the status of the site metric Metric Exchange connection at this GSLB site.
nwmetricmepstatus	<String>	Read-only	Indicates the status of the network metric Metric Exchange connection at this GSLB site.
sitetotalrequestbytes	<Double>	Read-only	Total number of request bytes received by the virtual servers represented by all GSLB services associated with this GSLB site.
siterequestbytesrate	<Double>	Read-only	Rate (/s) counter for sitetotalrequestbytes
sitetotalresponsebytes	<Double>	Read-only	Number of response bytes received by the virtual servers represented by all GSLB services associated with this GSLB site.
siteresponsebytesrate	<Double>	Read-only	Rate (/s) counter for sitetotalresponsebytes
sitetotalrequests	<Double>	Read-only	Total number of requests received by the virtual servers represented by all GSLB services

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			associated with this GSLB site.
siterequestsrate	<Double>	Read-only	Rate (/s) counter for sitetotalrequests
sitetotalresponses	<Double>	Read-only	Number of responses received by the virtual servers represented by all GSLB services associated with this GSLB site.
siteresponsesrate	<Double>	Read-only	Rate (/s) counter for sitetotalresponses
sitecurclntconnections	<Double>	Read-only	Number of current client connections to the virtual servers represented by all GSLB services associated with this GSLB site.
sitecursrvrconnections	<Double>	Read-only	Number of current connections to the real servers behind the virtual servers represented by all GSLB services associated with this GSLB site.

Operations

(click to see Properties)

- GET (ALL)
- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/gslbsite **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/gslbsite? **args=sitename: <String_value> ,detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get gslbsite resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/gslbsite? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "gslbsite": [ {

"sitename":<String_value>,

"siteipstr":<String_value>,

"nwmetricmepstatus":<String_value>,

"sitetype":<String_value>,

"sitemetricmepstatus":<String_value>,

"sitepublicip":<String_value>,

"sitetotalresponsebytes":<Double_value>,

"siteresponsesrate":<Double_value>,

"sitecursrvrconnections":<Double_value>,

"siterequestbytesrate":<Double_value>,

"sitepublicipstr":<String_value>,

"sitemetricexchange":<String_value>,

"siterequestsrate":<Double_value>,

"sitetotalrequests":<Double_value>,

"sitetotalresponses":<Double_value>,
```

```
"siteip":<String_value>,

"sitetotalrequestbytes":<Double_value>,

"nwmetricexchange":<String_value>,

"siteresponsebytesrate":<Double_value>,

"persexchange":<String_value>,

"sitecurclntconnections":<Double_value>,

"sitemepstatus":<String_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/stat/gslbsite/ sitename_value><String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "gslbsite": [ {

"sitename":<String_value>,

"siteipstr":<String_value>,
```

```
"nwmetricmepstatus":<String_value>,

"sitetype":<String_value>,

"sitemetricmepstatus":<String_value>,

"sitepublicip":<String_value>,

"sitetotalresponsebytes":<Double_value>,

"siteresponsesrate":<Double_value>,

"sitecursrvrconnections":<Double_value>,

"siterequestbytesrate":<Double_value>,

"sitepublicipstr":<String_value>,

"sitemetricexchange":<String_value>,

"siterequestsrate":<Double_value>,

"sitetotalrequests":<Double_value>,

"sitetotalresponses":<Double_value>,

"siteip":<String_value>,

"sitetotalrequestbytes":<Double_value>,

"nwmetricexchange":<String_value>,

"siteresponsebytesrate":<Double_value>,

"persexchange":<String_value>,

"sitecurclntconnections":<Double_value>,

"sitemepstatus":<String_value>

}]}
```

gslbvserver

Statistics for Global Server Load Balancing Virtual Server resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the GSLB virtual server for which to display statistics. If you do not specify a name, statistics are displayed for all GSLB virtual servers. Minimum length = 1
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full
establishedconn	<Double>	Read-only	Number of client connections in ESTABLISHED state.
inactsvcs	<Double>	Read-only	number of INACTIVE services bound to a vserver
vslbhealth	<Double>	Read-only	Health of the vserver. This gives percentage of UP services bound to this vserver.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
type	<String>	Read-only	Protocol associated with the vserver
state	<String>	Read-only	Current state of the server. There are seven possible values: UP(7), DOWN(1), UNKNOWN(2), BUSY(3), OFS(Out of Service)(4), TROFS(Transition Out of Service)(5), TROFS_DOWN(Down When going Out of Service)(8)
actsvcs	<Double>	Read-only	number of ACTIVE services bound to a vserver
tothits	<Double>	Read-only	Total vserver hits
hitsrate	<Double>	Read-only	Rate (/s) counter for tothits
vsvrtotbkplbhits	<Double>	Read-only	Total backup LB method hits
vsvrtotbkplbfail	<Double>	Read-only	Total backup LB method fails
curpersistencesessions	<Double>	Read-only	current vserver owned persistence sessions
vsvrtotpersistencehits	<Double>	Read-only	Total number of Persistence hits at vserver

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
totalrequestbytes	<Double>	Read-only	Total number of request bytes received on this service or virtual server.
requestbytesrate	<Double>	Read-only	Rate (/s) counter for totalrequestbytes
totalresponsebytes	<Double>	Read-only	Number of response bytes received by this service or virtual server.
responsebytesrate	<Double>	Read-only	Rate (/s) counter for totalresponsebytes
sothreshold	<Double>	Read-only	Spill Over Threshold set on the VServer.
totspillovers	<Double>	Read-only	Number of times vserver experienced spill over.
totvserverdownbackuphits	<Double>	Read-only	Number of times traffic was diverted to backup vserver since primary vserver was DOWN.
totalrequests	<Double>	Read-only	Total number of requests received on this service or virtual server. (This applies to HTTP/SSL services and servers.)
requestsrate	<Double>	Read-only	Rate (/s) counter for totalrequests

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
totalresponses	<Double>	Read-only	Number of responses received on this service or virtual server. (This applies to HTTP/SSL services and servers.)
responsesrate	<Double>	Read-only	Rate (/s) counter for totalresponses
curclntconnections	<Double>	Read-only	Number of current client connections.
cursrvrconnections	<Double>	Read-only	Number of current connections to the actual servers behind the virtual server.

Operations

(click to see Properties)

- GET (ALL)
- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of

creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/gslbvserver **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/gslbvserver? **args=name: <String_value> ,detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get gslbvserver resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/gslbvserver? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "gslbvserver": [ {

"name":<String_value>,

"vsvrtotbkplbhits":<Double_value>,

"cursrvrconnections":<Double_value>,

"totalresponses":<Double_value>,

"requestbytesrate":<Double_value>,

"totalresponsebytes":<Double_value>,

"hitsrate":<Double_value>,

"establishedconn":<Double_value>,

"inactsvcs":<Double_value>,

"state":<String_value>,

"actsvcs":<Double_value>,

"type":<String_value>,

"totspillovers":<Double_value>,

"responsebytesrate":<Double_value>,

"curclntconnections":<Double_value>,

"totvserverdownbackuphits":<Double_value>,

"requestsrate":<Double_value>,

"curpersistencesessions":<Double_value>,

"totalrequestbytes":<Double_value>,

"sothreshold":<Double_value>,
```

```
"tothits":<Double_value>,

"vslbhealth":<Double_value>,

"totalrequests":<Double_value>,

"responsesrate":<Double_value>,

"vsvrtotpersistencehits":<Double_value>,

"vsvrtotbkplbfail":<Double_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/stat/gslbvserver/ name_value><String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "gslbvserver": [ {

"name":<String_value>,

"vsvrtotbkplbhits":<Double_value>,

"cursrvrconnections":<Double_value>,
```

```
"totalresponses":<Double_value>,

"requestbytesrate":<Double_value>,

"totalresponsebytes":<Double_value>,

"hitsrate":<Double_value>,

"establishedconn":<Double_value>,

"inactsvcs":<Double_value>,

"state":<String_value>,

"actsvcs":<Double_value>,

"type":<String_value>,

"totspillovers":<Double_value>,

"responsebytesrate":<Double_value>,

"curclntconnections":<Double_value>,

"totvserverdownbackuphits":<Double_value>,

"requestsrate":<Double_value>,

"curpersistencesessions":<Double_value>,

"totalrequestbytes":<Double_value>,

"sothreshold":<Double_value>,

"tothits":<Double_value>,

"vslbhealth":<Double_value>,

"totalrequests":<Double_value>,

"responsesrate":<Double_value>,

"vsvrtotpersistencehits":<Double_value>,
```

```
"vsvrtotbkplbfail":<Double_value>

}]}
```

ha

High Availability

High-availability commands.

NAME	DESCRIPTION
hanode	Statistics for node resource.

hanode

Statistics for node resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full
hacurstatus	<String>	Read-only	Whether a Citrix ADC is configured for high availability. Possible values are YES and NO. If the value is NO, the high availability statistics below are invalid.
hacurstate	<String>	Read-only	State of the HA node, based on its health, in a high

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			availability setup. Possible values are: UP - Indicates that the node is accessible and can function as either a primary or secondary node. DISABLED - Indicates that the high availability status of the node has been manually disabled. Synchronization and propagation cannot take place between the peer nodes. INIT - Indicates that the node is in the process of becoming part of the high availability configuration. PARTIALFAIL - Indicates that one of the high availability monitored interfaces has failed because of a card or link failure. This state triggers a failover. COMPLETEFAIL - Indicates that all the interfaces of the node are unusable, because the interfaces on which high availability monitoring is enabled are not connected or are

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			manually disabled. This state triggers a failover. DUMB - Indicates that the node is in listening mode. It does not participate in high availability transitions or transfer configuration from the peer node. This is a configured value, not a statistic. PARTIALFAILSSL - Indicates that the SSL card has failed. This state triggers a failover. ROUTEMONITORFAIL - Indicates that the route monitor has failed. This state triggers a failover.
hacurmasterstate	<String>	Read-only	Indicates the high availability state of the node. Possible values are: STAYSECONDARY - Indicates that the selected node remains the secondary node in a high availability setup. In this case a forced failover does not change the state but, instead, returns an appropriate error message. This is a configured value and

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			not a statistic. PRIMARY - Indicates that the selected node is the primary node in a high availability setup. SECONDARY - Indicates that the selected node is the secondary node in a high availability setup. CLAIMING - Indicates that the secondary node is in the process of taking over as the primary node. This is the intermediate state in the transition of the secondary node to primary status. FORCE CHANGE - Indicates that the secondary node is forcibly changing its status to primary due to a forced failover issued on the secondary node.
transtime	<String>	Read-only	Time when the last master state transition occurred. You can use this statistic for debugging.
hatotpktrx	<Double>	Read-only	Number of heartbeat packets received from the peer node. Heartbeats are sent

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			at regular intervals (default is 200 milliseconds) to determine the state of the peer node.
hapktrxrate	<Double>	Read-only	Rate (/s) counter for hatotpktrx
hatotpkttx	<Double>	Read-only	Number of heartbeat packets sent to the peer node. Heartbeats are sent at regular intervals (default is 200 milliseconds) to determine the state of the peer node.
hapkttxrate	<Double>	Read-only	Rate (/s) counter for hatotpkttx
haerrproptimeout	<Double>	Read-only	Number of times propagation timed out.
haerrsyncfailure	<Double>	Read-only	Number of times the configuration of the primary and secondary nodes failed to synchronize since that last transition. A synchronization failure results in mismatched configuration. It can be caused by a mismatch in the Remote Procedural Call (RPC) password on the two nodes

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			forming the high availability pair.

Operations

(click to see Properties)

- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/hanode **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/hanode? **args=detail: <Boolean_value> ,fullvalues:**

<Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>

Use this query-parameter to get hanode resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/hanode? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "hanode": [ {

"hacurmasterstate":<String_value>,

"haerrproptimeout":<Double_value>,

"hapkttxrate":<Double_value>,

"hacurstate":<String_value>,

"hacurstatus":<String_value>,

"hatotpkttx":<Double_value>,

"hatotpktrx":<Double_value>,

"haerrsyncfailure":<Double_value>,
```

```
"hapktrxrate":<Double_value>,

"transtime":<String_value>

}]}
```

ica

Ica

ICA statistics.

NAME	DESCRIPTION
icapolicy	Statistics for ICA policy resource.

icapolicy

Statistics for ICA policy resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the ica policy. Minimum length = 1
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full
pipolicyhits	<Double>	Read-only	Number of hits on the policy
pipolicyhitsrate	<Double>	Read-only	Rate (/s) counter for pipolicyhits

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
pipolicyundefhits	<Double>	Read-only	Number of undef hits on the policy
pipolicyundefhitsrate	<Double>	Read-only	Rate (/s) counter for pipolicyundefhits

Operations

(click to see Properties)

- GET (ALL)
- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/icapolicy **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/icapolicy? **args=name: <String_value> ,detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get icapolicy resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/icapolicy? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "icapolicy": [ {

"name":<String_value>,

"pipolicyundefhits":<Double_value>,

"pipolicyhits":<Double_value>,

"pipolicyundefhitsrate":<Double_value>,

"pipolicyhitsrate":<Double_value>
```

```
}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/stat/icapolicy/ name_value><String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "icapolicy": [ {

"name":<String_value>,

"pipolicyundefhits":<Double_value>,

"pipolicyhits":<Double_value>,

"pipolicyundefhitsrate":<Double_value>,

"pipolicyhitsrate":<Double_value>

}]}
```

ipsec

Ipsec

IPSEC statistics.

NAME	DESCRIPTION
ipseccounters	Statistics for counters resource.

ipseccounters

Statistics for counters resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full
ipsectotrxbytes	<Double>	Read-only	Bytes received during IPsec sessions.
ipsecrxbytesrate	<Double>	Read-only	Rate (/s) counter for ipsectotrxbytes
ipsectottxbytes	<Double>	Read-only	Bytes sent during IPsec sessions.
ipsectxbytesrate	<Double>	Read-only	Rate (/s) counter for ipsectottxbytes
ipsectotrxpkts	<Double>	Read-only	Packets received during IPsec sessions.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ipsecrxpktsrate	<Double>	Read-only	Rate (/s) counter for ipsectotrxpkts
ipsectottxpkts	<Double>	Read-only	Packets sent during IPsec sessions.
ipsectxpktsrate	<Double>	Read-only	Rate (/s) counter for ipsectottxpkts

Operations

(click to see Properties)

- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/ipseccounters **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/ipseccounters? **args=detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get ipseccounters resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/ipseccounters? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "ipseccounters": [ {

"ipsectxbytesrate":<Double_value>,

"ipsectotrxpkts":<Double_value>,

"ipsectxpktsrate":<Double_value>,

"ipsectottxpkts":<Double_value>,

"ipsecrxpktsrate":<Double_value>,
```

```
"ipsectottxbytes":<Double_value>,

"ipsectotrxbytes":<Double_value>,

"ipsecrxbytesrate":<Double_value>

}]}
```

ipsecalg

Ipsecalg

IPSECALG statistics.

NAME	DESCRIPTION
ipsecalgcounters	Statistics for counters resource.

ipsecalgcounters

Statistics for counters resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of IPSec ALG Profile. Minimum length = 1 Maximum length = 32
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ipsecalgtotsessions	<Double>	Read-only	Total session for IPSec ALG.
ipsecalgsessionsrate	<Double>	Read-only	Rate (/s) counter for ipsecalgtotsessions
ipsecalgtotdrsessions	<Double>	Read-only	Total Dropped IPsec ALG sessions.
ipsecalgdrsessionsrate	<Double>	Read-only	Rate (/s) counter for ipsecalgtotdrsessions
ipsecalgcuractsessions	<Double>	Read-only	Currently active IPsec ALG sessions.
ipsecalgcuractsessionsrate	<Double>	Read-only	Rate (/s) counter for ipsecalgcuractsessions
ipsecalgcurblksessions	<Double>	Read-only	Currently blocked sessions on ESP Gate.
ipsecalgcurblksessionsrate	<Double>	Read-only	Rate (/s) counter for ipsecalgcurblksessions
ipsecalgtotrxpkts	<Double>	Read-only	Total Packets received during IPsec ALG sessions.
ipsecalgrxpktsrate	<Double>	Read-only	Rate (/s) counter for ipsecalgtotrxpkts
ipsecalgtottxpkts	<Double>	Read-only	Total Packets sent during IPsec ALG sessions.
ipsecalgtxpktsrate	<Double>	Read-only	Rate (/s) counter for ipsecalgtottxpkts

Operations

(click to see Properties)

- GET (ALL)
- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/ipsecalgcounters **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/ipsecalgcounters? **args=name: <String_value> ,detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get ipsecalgcounters resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/ipsecalgcounters? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "ipsecalgcounters": [ {

"name":<String_value>,

"ipsecalgrxpktsrate":<Double_value>,

"ipsecalgtotdrsessions":<Double_value>,

"ipsecalgtxpktsrate":<Double_value>,

"ipsecalgtotrxpkts":<Double_value>,

"ipsecalgcurblksessionsrate":<Double_value>,

"ipsecalgcuractsessions":<Double_value>,

"ipsecalgcurblksessions":<Double_value>,

"ipsecalgcuractsessionsrate":<Double_value>,
```

```
"ipsecalgdrsessionsrate":<Double_value>,

"ipsecalgsessionsrate":<Double_value>,

"ipsecalgtottxpkts":<Double_value>,

"ipsecalgtotsessions":<Double_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/stat/ipsecalgcounters/ name_value><String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "ipsecalgcounters": [ {

"name":<String_value>,

"ipsecalgrxpktsrate":<Double_value>,

"ipsecalgtotdrsessions":<Double_value>,

"ipsecalgtxpktsrate":<Double_value>,

"ipsecalgtotrxpkts":<Double_value>,
```

```
"ipsecalgcurblksessionsrate":<Double_value>,

"ipsecalgcuractsessions":<Double_value>,

"ipsecalgcurblksessions":<Double_value>,

"ipsecalgcuractsessionsrate":<Double_value>,

"ipsecalgdrsessionsrate":<Double_value>,

"ipsecalgsessionsrate":<Double_value>,

"ipsecalgtottxpkts":<Double_value>,

"ipsecalgtotsessions":<Double_value>

}]}
```

lb

Load Balancing

Load Balancing statistics. The load balancing methods manage the selection of an appropriate physical server in a server farm.

NAME	DESCRIPTION
lbpolicy	Statistics for lb policy resource.
lbpolicylabel	Statistics for lb policy label resource.
lbvserver	Statistics for Load Balancing Virtual Server resource.

lbpolicy

Statistics for lb policy resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the LB policy for which to show detailed statistics. Minimum length = 1
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full
pipolicyhits	<Double>	Read-only	Number of hits on the policy
pipolicyhitsrate	<Double>	Read-only	Rate (/s) counter for pipolicyhits
pipolicyundefhits	<Double>	Read-only	Number of undef hits on the policy
pipolicyundefhitsrate	<Double>	Read-only	Rate (/s) counter for pipolicyundefhits

Operations

(click to see Properties)

- GET (ALL)
- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/lbpolicy **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/lbpolicy? **args=name: <String_value> ,detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get lbpolicy resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/lbpolicy? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lbpolicy": [ {

"name":<String_value>,

"pipolicyhits":<Double_value>,

"pipolicyundefhits":<Double_value>,

"pipolicyhitsrate":<Double_value>,

"pipolicyundefhitsrate":<Double_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/stat/lbpolicy/ name_value><String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lbpolicy": [ {

"name":<String_value>,

"pipolicyhits":<Double_value>,

"pipolicyundefhits":<Double_value>,

"pipolicyhitsrate":<Double_value>,

"pipolicyundefhitsrate":<Double_value>

}]}
```

lbpolicylabel

Statistics for lb policy label resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
labelname	<String>	Read-write	Name of the LB policy label. Minimum length = 1
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full
pipolicylabelhits	<Double>	Read-only	Number of times policy label was invoked.
pipolicylabelhitsrate	<Double>	Read-only	Rate (/s) counter for pipolicylabelhits

Operations

(click to see Properties)

- GET (ALL)
- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/lbpolicylabel **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/lbpolicylabel? **args=labelname: <String_value> ,detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get lbpolicylabel resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/lbpolicylabel? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lbpolicylabel": [ {

"labelname":<String_value>,

"pipolicylabelhits":<Double_value>,

"pipolicylabelhitsrate":<Double_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/stat/lbpolicylabel/ labelname_value><String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lbpolicylabel": [ {

"labelname":<String_value>,

"pipolicylabelhits":<Double_value>,

"pipolicylabelhitsrate":<Double_value>

}]}
```

lbvserver

Statistics for Load Balancing Virtual Server resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the virtual server. If no name is provided, statistical data of all configured virtual servers is displayed. Minimum length = 1
clearstats	<String>	Read-write	Clear the statsistics / counters.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = basic, full
sortby	<String>	Read-write	use this argument to sort by specific key. Possible values = Hits, CPU-PM
sortorder	<String>	Read-write	use this argument to specify sort order. Default value: SORT_DESCENDING Possible values = ascending, descending
avgcltttlb	<Double>	Read-only	Average TTLB between the client and the server. TTLB is the time interval between sending the request packet to a service and receiving the ACK for response from client.
cltresponsetimeapdex	<Double>	Read-only	Vserver APDEX index based on client response times.
vsvrsurgecount	<Double>	Read-only	Number of requests waiting on this vserver.
establishedconn	<Double>	Read-only	Number of client connections in ESTABLISHED state.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
inactsvcs	<Double>	Read-only	number of INACTIVE services bound to a vserver
vslbhealth	<Double>	Read-only	Health of the vserver. This gives percentage of UP services bound to this vserver.
primaryipaddress	<String>	Read-only	IP address of the vserver
primaryport	<Integer>	Read-only	The port on which the service is running.
type	<String>	Read-only	Protocol associated with the vserver
state	<String>	Read-only	Current state of the server. There are seven possible values: UP(7), DOWN(1), UNKNOWN(2), BUSY(3), OFS(Out of Service)(4), TROFS(Transition Out of Service)(5), TROFS_DOWN(Down When going Out of Service)(8)
actsvcs	<Double>	Read-only	number of ACTIVE services bound to a vserver
cpuusagepm	<Double>	Read-only	Vserver CPU usage in per-mille(parts per thousand)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
tothits	<Double>	Read-only	Total vserver hits
hitsrate	<Double>	Read-only	Rate (/s) counter for tothits
totalrequests	<Double>	Read-only	Total number of requests received on this service or virtual server. (This applies to HTTP/SSL services and servers.)
requestsrate	<Double>	Read-only	Rate (/s) counter for totalrequests
totalresponses	<Double>	Read-only	Number of responses received on this service or virtual server. (This applies to HTTP/SSL services and servers.)
responsesrate	<Double>	Read-only	Rate (/s) counter for totalresponses
totalrequestbytes	<Double>	Read-only	Total number of request bytes received on this service or virtual server.
requestbytesrate	<Double>	Read-only	Rate (/s) counter for totalrequestbytes
totalresponsebytes	<Double>	Read-only	Number of response bytes received by this service or virtual server.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
responsebytesrate	<Double>	Read-only	Rate (/s) counter for totalresponsebytes
totalh2requests	<Double>	Read-only	Total number of Http2 requests received on this service or virtual server. (This applies to HTTP/SSL services and servers.)
h2requestsrate	<Double>	Read-only	Rate (/s) counter for totalh2requests
totalh2responses	<Double>	Read-only	Number of Http2 responses received on this service or virtual server. (This applies to HTTP/SSL services and servers.)
h2responsesrate	<Double>	Read-only	Rate (/s) counter for totalh2responses
totalpktsrecvd	<Double>	Read-only	Total number of packets received by this service or virtual server.
pktsrecvdrate	<Double>	Read-only	Rate (/s) counter for totalpktsrecvd
totalpktssent	<Double>	Read-only	Total number of packets sent.
pktssentrate	<Double>	Read-only	Rate (/s) counter for totalpktssent

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
curclntconnections	<Double>	Read-only	Number of current client connections.
cursrvrconnections	<Double>	Read-only	Number of current connections to the actual servers behind the virtual server.
curpersistencesessions	<Double>	Read-only	current vserver owned persistence sessions
curbackuppersistencesessions	<Double>	Read-only	current vserver owned backup persistence sessions
surgecount	<Double>	Read-only	Number of requests in the surge queue.
svcsurgecount	<Double>	Read-only	Total number of requests in the surge queues of all the services bound to this LB-vserver.
sothreshold	<Double>	Read-only	Spill Over Threshold set on the VServer.
totspillovers	<Double>	Read-only	Number of times vserver experienced spill over.
labelledconn	<Double>	Read-only	Number of Labeled connection on this vserver
pushlabel	<Double>	Read-only	Number of labels for this push vserver.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
deferredreq	<Double>	Read-only	Number of deferred request on this vserver
deferredreqrate	<Double>	Read-only	Rate (/s) counter for deferredreq
invalidrequestrespon se	<Double>	Read-only	Number invalid requests/responses on this vserver
invalidrequestrespon sedropped	<Double>	Read-only	Number invalid requests/responses dropped on this vserver
totvserverdownbacku phits	<Double>	Read-only	Number of times traffic was diverted to backup vserver since primary vserver was DOWN.
curmptcpsessions	<Double>	Read-only	Current Multipath TCP sessions
cursubflowconn	<Double>	Read-only	Current Multipath TCP subflows
totalconnreassembly queue75	<Double>	Read-only	Total no of connections with 75% TCP reassembly queue
totalconnreassembly queueflush	<Double>	Read-only	Total no of connections incurred TCP reassembly queue flush
totalsvrbusyerr	<Double>	Read-only	Total no of server busy error

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
svrbusyerrrate	<Double>	Read-only	Rate (/s) counter for totalsvrbusyerr
reqretrycount	<Double>	Read-only	Number of times request has been retried due to server failure.
reqretrycountexceeded	<Double>	Read-only	Number of times Maximum retry count threshold is exceeded and error returned to client.
httpmaxhdrszpkts	<Double>	Read-only	Number of http max header size packet parsing failures
httpmaxhdrfldlenpkts	<Double>	Read-only	Number of HTTP requests exceeding max header field length
tcpmaxooopkts	<Double>	Read-only	No of times max out of order packets reached
totclttlbtransactions	<Double>	Read-only	Total transactions where client TTLB is calculated.
toleratingttlbtransactions	<Double>	Read-only	Tolerable transactions based on APDEX threshold (>T ;; <4T).
frustratingttlbtransactions	<Double>	Read-only	Frustrating transactions based on APDEX threshold (>4T).

Operations

(click to see Properties)

- GET (ALL)
- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/lbvserver **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/lbvserver? **args=name: <String_value> ,detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value> ,sortby: <String_value> ,sortorder: <String_value> ,sortorder: <String_value>**

Use this query-parameter to get lbvserver resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/lbvserver? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lbvserver": [ {

"name":<String_value>,

"totalrequests":<Double_value>,

"responsesrate":<Double_value>,

"curmptcpsessions":<Double_value>,

"avgclttlb":<Double_value>,

"pushlabel":<Double_value>,

"totalh2responses":<Double_value>,

"cltresponsetimeapdex":<Double_value>,

"totvserverdownbackuphits":<Double_value>,
```

```
"vsvrsurgecount":<Double_value>,

"requestsrate":<Double_value>,

"deferredreq":<Double_value>,

"totclttlbtransactions":<Double_value>,

"svcsurgecount":<Double_value>,

"totalpktssent":<Double_value>,

"h2requestsrate":<Double_value>,

"curpersistencesessions":<Double_value>,

"primaryport":<Integer_value>,

"sothreshold":<Double_value>,

"totalrequestbytes":<Double_value>,

"invalidrequestresponse":<Double_value>,

"pktssentrate":<Double_value>,

"vslbhealth":<Double_value>,

"tothits":<Double_value>,

"reqretrycount":<Double_value>,

"frustratingttlbtransactions":<Double_value>,

"toleratingttlbtransactions":<Double_value>,

"actsvcs":<Double_value>,

"state":<String_value>,

"totalconnreassemblyqueue75":<Double_value>,

"svrbusyerrrate":<Double_value>,
```

```
"httpmaxhdrfldlenpkts":<Double_value>,

"type":<String_value>,

"deferredreqrate":<Double_value>,

"totalh2requests":<Double_value>,

"totalconnreassemblyqueueflush":<Double_value>,

"totspillovers":<Double_value>,

"curclntconnections":<Double_value>,

"responsebytesrate":<Double_value>,

"totalpktsrecvd":<Double_value>,

"surgecount":<Double_value>,

"labelledconn":<Double_value>,

"tcpmaxooopkts":<Double_value>,

"cursrvrconnections":<Double_value>,

"invalidrequestresponsedropped":<Double_value>,

"cursubflowconn":<Double_value>,

"curbackuppersistencesessions":<Double_value>,

"cpuusagepm":<Double_value>,

"totalresponses":<Double_value>,

"h2responsesrate":<Double_value>,

"requestbytesrate":<Double_value>,

"pktsrecvdrate":<Double_value>,

"hitsrate":<Double_value>,
```

```
"totalresponsebytes":<Double_value>,

"reqretrycountexceeded":<Double_value>,

"totalsvrbusyerr":<Double_value>,

"establishedconn":<Double_value>,

"primaryipaddress":<String_value>,

"httpmaxhdrszpkts":<Double_value>,

"inactsvcs":<Double_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/stat/lbvserver/ name_value><String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lbvserver": [ {

"name":<String_value>,

"totalrequests":<Double_value>,
```

```
"responsesrate":<Double_value>,

"curmptcpsessions":<Double_value>,

"avgclttlb":<Double_value>,

"pushlabel":<Double_value>,

"totalh2responses":<Double_value>,

"cltresponsetimeapdex":<Double_value>,

"totvserverdownbackuphits":<Double_value>,

"vsvrsurgecount":<Double_value>,

"requestsrate":<Double_value>,

"deferredreq":<Double_value>,

"totclttlbtransactions":<Double_value>,

"svcsurgecount":<Double_value>,

"totalpktssent":<Double_value>,

"h2requestsrate":<Double_value>,

"curpersistencesessions":<Double_value>,

"primaryport":<Integer_value>,

"sothreshold":<Double_value>,

"totalrequestbytes":<Double_value>,

"invalidrequestresponse":<Double_value>,

"pktssentrate":<Double_value>,

"vslbhealth":<Double_value>,

"tothits":<Double_value>,
```

```
"reqretrycount":<Double_value>,

"frustratingttlbtransactions":<Double_value>,

"toleratingttlbtransactions":<Double_value>,

"actsvcs":<Double_value>,

"state":<String_value>,

"totalconnreassemblyqueue75":<Double_value>,

"svrbusyerrrate":<Double_value>,

"httpmaxhdrfldlenpkts":<Double_value>,

"type":<String_value>,

"deferredreqrate":<Double_value>,

"totalh2requests":<Double_value>,

"totalconnreassemblyqueueflush":<Double_value>,

"totspillovers":<Double_value>,

"curclntconnections":<Double_value>,

"responsebytesrate":<Double_value>,

"totalpktsrecvd":<Double_value>,

"surgecount":<Double_value>,

"labelledconn":<Double_value>,

"tcpmaxooopkts":<Double_value>,

"cursrvrconnections":<Double_value>,

"invalidrequestresponsedropped":<Double_value>,

"cursubflowconn":<Double_value>,
```

```
"curbackuppersistencesessions":<Double_value>,

"cpuusagepm":<Double_value>,

"totalresponses":<Double_value>,

"h2responsesrate":<Double_value>,

"requestbytesrate":<Double_value>,

"pktsrecvdrate":<Double_value>,

"hitsrate":<Double_value>,

"totalresponsebytes":<Double_value>,

"reqretrycountexceeded":<Double_value>,

"totalsvrbusyerr":<Double_value>,

"establishedconn":<Double_value>,

"primaryipaddress":<String_value>,

"httpmaxhdrszpkts":<Double_value>,

"inactsvcs":<Double_value>

}]}
```

lldp

LLDP

Link Layer Discovery Protocol.

NAME	DESCRIPTION
lldp	Statistics for lldp.

lldp

Statistics for lldp.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ifnum	<String>	Read-write	LLDP Statistics per interfaces.
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full
rxportframestotal	<Double>	Read-only	Total LLDP Packets received.
rxportframesrate	<Double>	Read-only	Rate (/s) counter for rxportframestotal
rxportbytestotal	<Double>	Read-only	Total LLDP bytes received
rxportbytesrate	<Double>	Read-only	Rate (/s) counter for rxportbytestotal
txportframestotal	<Double>	Read-only	Total LLDP Packets transmitted
txportframesrate	<Double>	Read-only	Rate (/s) counter for txportframestotal
txportbytestotal	<Double>	Read-only	Total LLDP bytes transmitted.
txportbytesrate	<Double>	Read-only	Rate (/s) counter for txportbytestotal
rxportframeserrors	<Double>	Read-only	Total errors in LLDP packets.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
rxportframeserrorsrate	<Double>	Read-only	Rate (/s) counter for rxportframeserrors
rxporttlvsdiscardedtotal	<Double>	Read-only	Total discarded LLDP packets.
rxporttlvsdiscardedrate	<Double>	Read-only	Rate (/s) counter for rxporttlvsdiscardedtotal
rxporttlvsunrecognizedtotal	<Double>	Read-only	Total TLVs not Recognised.
rxporttlvsunrecognizedrate	<Double>	Read-only	Rate (/s) counter for rxporttlvsunrecognizedtotal

Operations

(click to see Properties)

- GET (ALL)
- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/lldp **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/lldp? **args=ifnum: <String_value> ,detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get lldp resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/lldp? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lldp": [ {

"ifnum":<String_value>,
```

```
"txportbytestotal":<Double_value>,

"txportbytesrate":<Double_value>,

"rxporttlvsdiscardedtotal":<Double_value>,

"rxporttlvsdiscardedrate":<Double_value>,

"rxportbytestotal":<Double_value>,

"rxportframeserrorsrate":<Double_value>,

"rxportbytesrate":<Double_value>,

"rxporttlvsunrecognizedtotal":<Double_value>,

"rxportframestotal":<Double_value>,

"rxportframesrate":<Double_value>,

"rxportframeserrors":<Double_value>,

"rxporttlvsunrecognizedrate":<Double_value>,

"txportframestotal":<Double_value>,

"txportframesrate":<Double_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/stat/lldp/ ifnum_value><String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lldp": [ {

"ifnum":<String_value>,

"txportbytestotal":<Double_value>,

"txportbytesrate":<Double_value>,

"rxporttlvsdiscardedtotal":<Double_value>,

"rxporttlvsdiscardedrate":<Double_value>,

"rxportbytestotal":<Double_value>,

"rxportframeserrorsrate":<Double_value>,

"rxportbytesrate":<Double_value>,

"rxporttlvsunrecognizedtotal":<Double_value>,

"rxportframestotal":<Double_value>,

"rxportframesrate":<Double_value>,

"rxportframeserrors":<Double_value>,

"rxporttlvsunrecognizedrate":<Double_value>,

"txportframestotal":<Double_value>,

"txportframesrate":<Double_value>

}]}
```

lsn

Lsn

Large Scale NAT commands

NAME	DESCRIPTION
lsn	Statistics for lsn.
lsndslite	
lsngroup	Statistics for LSN group resource.
lsnnat64	
lsnpool	Statistics for LSN pool resource.

lsn

Statistics for lsn.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full
lsntottcprxpkts	<Double>	Read-only	Number of LSN TCP Received packets.
lsntcprxpktsrate	<Double>	Read-only	Rate (/s) counter for lsntottcprxpkts
lsntottcprxbytes	<Double>	Read-only	Number of LSN TCP Received bytes.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
lsntcprxbytesrate	<Double>	Read-only	Rate (/s) counter for lsntottcprxbytes
lsntottcptxpkts	<Double>	Read-only	Number of LSN TCP Transmitted packets.
lsntcptxpktsrate	<Double>	Read-only	Rate (/s) counter for lsntottcptxpkts
lsntottcptxbytes	<Double>	Read-only	Number of LSN TCP Transmitted bytes.
lsntcptxbytesrate	<Double>	Read-only	Rate (/s) counter for lsntottcptxbytes
lsntottcpdrppkts	<Double>	Read-only	Number of LSN TCP Dropped packets.
lsntcpdrppktsrate	<Double>	Read-only	Rate (/s) counter for lsntottcpdrppkts
lsncurtcpsessions	<Double>	Read-only	Number of LSN TCP Current Sessions.
lsncurtcpsessionsrate	<Double>	Read-only	Rate (/s) counter for lsncurtcpsessions
lsntotudprxpkts	<Double>	Read-only	Number of LSN UDP Received packets.
lsnudprxpktsrate	<Double>	Read-only	Rate (/s) counter for lsntotudprxpkts
lsntotudprxbytes	<Double>	Read-only	Number of LSN UDP Received bytes.
lsnudprxbytesrate	<Double>	Read-only	Rate (/s) counter for lsntotudprxbytes
lsntotudptxpkts	<Double>	Read-only	Number of LSN UDP Transmitted packets.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
lsnudptxpktsrate	<Double>	Read-only	Rate (/s) counter for lsntotudptxpkts
lsntotudptxbytes	<Double>	Read-only	Number of LSN UDP Transmitted bytes.
lsnudptxbytesrate	<Double>	Read-only	Rate (/s) counter for lsntotudptxbytes
lsntotudpdrppkts	<Double>	Read-only	Number of LSN UDP Dropped packets.
lsnudpdrppktsrate	<Double>	Read-only	Rate (/s) counter for lsntotudpdrppkts
lsncurudpsessions	<Double>	Read-only	Number of LSN UDP Current Sessions.
lsncurudpsessionsrate	<Double>	Read-only	Rate (/s) counter for lsncurudpsessions
lsntoticmprxpkts	<Double>	Read-only	Number of LSN ICMP Received packets.
lsnicmprxpktsrate	<Double>	Read-only	Rate (/s) counter for lsntoticmprxpkts
lsntoticmprxbytes	<Double>	Read-only	Number of LSN ICMP Received bytes.
lsnicmprxbytesrate	<Double>	Read-only	Rate (/s) counter for lsntoticmprxbytes
lsntoticmptxpkts	<Double>	Read-only	Number of LSN ICMP Transmitted packets.
lsnicmptxpktsrate	<Double>	Read-only	Rate (/s) counter for lsntoticmptxpkts

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
lsntoticmptxbytes	<Double>	Read-only	Number of LSN ICMP Transmitted bytes.
lsnicmptxbytesrate	<Double>	Read-only	Rate (/s) counter for lsntoticmptxbytes
lsntoticmpdrppkts	<Double>	Read-only	Number of LSN ICMP Dropped packets.
lsnicmpdrppktsrate	<Double>	Read-only	Rate (/s) counter for lsntoticmpdrppkts
lsncuricmpsessions	<Double>	Read-only	Number of LSN ICMP Current Sessions.
lsncuricmpsessionsrate	<Double>	Read-only	Rate (/s) counter for lsncuricmpsessions
lsncursessions	<Double>	Read-only	Current number of LSN sessions.
lsncursessionsrate	<Double>	Read-only	Rate (/s) counter for lsncursessions
lsncursubscribers	<Double>	Read-only	Current number of LSN subscribers.
lsncursubscribersrate	<Double>	Read-only	Rate (/s) counter for lsncursubscribers

Operations

(click to see Properties)

- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/lsn **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/lsn? **args=detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get lsn resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/lsn? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lsn": [ {

"lsntotudptxpkts":<Double_value>,

"lsntotudprxpkts":<Double_value>,

"lsntotudptxbytes":<Double_value>,

"lsntotudprxbytes":<Double_value>,

"lsncursubscribersrate":<Double_value>,

"lsnudptxpktsrate":<Double_value>,

"lsntoticmptxpkts":<Double_value>,

"lsncurtcpsessions":<Double_value>,

"lsncursessions":<Double_value>,

"lsnudptxbytesrate":<Double_value>,

"lsntcpdrppktsrate":<Double_value>,

"lsncuricmpsessions":<Double_value>,

"lsntcprxbytesrate":<Double_value>,

"lsntottcpdrppkts":<Double_value>,

"lsncurtcpsessionsrate":<Double_value>,
```

```
"lsncursessionsrate":<Double_value>,

"lsncursubscribers":<Double_value>,

"lsntoticmprxpkts":<Double_value>,

"lsntcprxpktsrate":<Double_value>,

"lsntcptxpktsrate":<Double_value>,

"lsnicmprxbytesrate":<Double_value>,

"lsntottcptxbytes":<Double_value>,

"lsnicmpdrppktsrate":<Double_value>,

"lsntottcprxbytes":<Double_value>,

"lsntottcptxpkts":<Double_value>,

"lsnicmptxpktsrate":<Double_value>,

"lsntottcprxpkts":<Double_value>,

"lsntcptxbytesrate":<Double_value>,

"lsncurudpsessions":<Double_value>,

"lsntoticmprxbytes":<Double_value>,

"lsnudpdrppktsrate":<Double_value>,

"lsntoticmptxbytes":<Double_value>,

"lsnudprxbytesrate":<Double_value>,

"lsncuricmpsessionsrate":<Double_value>,

"lsnicmptxbytesrate":<Double_value>,

"lsncurudpsessionsrate":<Double_value>,

"lsntotudpdrppkts":<Double_value>,
```

```
"lsntoticmpdrppkts":<Double_value>,

"lsnicmprxpktsrate":<Double_value>,

"lsnudprxpktsrate":<Double_value>

}]}
```

lsndslite

Read/write properties

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full
lsntotdsliterxpkts	<Double>	Read-only	Total number of LSN DS-Lite rx pkts.
lsndsliterxpktsrate	<Double>	Read-only	Rate (/s) counter for lsntotdsliterxpkts
lsntotdsliterxbytes	<Double>	Read-only	Total number of LSN DS-Lite rx bytes.
lsndsliterxbytesrate	<Double>	Read-only	Rate (/s) counter for lsntotdsliterxbytes
lsntotdslitetxpkts	<Double>	Read-only	Total number of LSN DS-Lite tx pkts.
lsndslitetxpktsrate	<Double>	Read-only	Rate (/s) counter for lsntotdslitetxpkts

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
lsntotdslitetxbytes	<Double>	Read-only	Total number of LSN DS-Lite tx bytes.
lsndslitetxbytesrate	<Double>	Read-only	Rate (/s) counter for lsntotdslitetxbytes
lsntotdslitetcprxpkts	<Double>	Read-only	Number of LSN DS-Lite TCP Received packets.
lsndslitetcprxpktsrate	<Double>	Read-only	Rate (/s) counter for lsntotdslitetcprxpkts
lsntotdslitetcprxbytes	<Double>	Read-only	Number of LSN DS-Lite TCP Received bytes.
lsndslitetcprxbytesrate	<Double>	Read-only	Rate (/s) counter for lsntotdslitetcprxbytes
lsntotdslitetcptxpkts	<Double>	Read-only	Number of LSN DS-Lite TCP Transmitted packets.
lsndslitetcptxpktsrate	<Double>	Read-only	Rate (/s) counter for lsntotdslitetcptxpkts
lsntotdslitetcptxbytes	<Double>	Read-only	Number of LSN DS-Lite TCP Transmitted bytes.
lsndslitetcptxbytesrate	<Double>	Read-only	Rate (/s) counter for lsntotdslitetcptxbytes
lsntotdslitetcpdrppkts	<Double>	Read-only	Number of LSN DS-Lite TCP Dropped packets.
lsndslitetcpdrppktsrate	<Double>	Read-only	Rate (/s) counter for lsntotdslitetcpdrppkts

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
lsncurdslitetcpsessions	<Double>	Read-only	Number of LSN DS-Lite TCP Current Sessions.
lsncurdslitetcpsessionsrate	<Double>	Read-only	Rate (/s) counter for lsncurdslitetcpsessions
lsntotdsliteudprxpkts	<Double>	Read-only	Number of LSN DS-Lite UDP Received packets.
lsndsliteudprxpktsrate	<Double>	Read-only	Rate (/s) counter for lsntotdsliteudprxpkts
lsntotdsliteudprxbytes	<Double>	Read-only	Number of LSN DS-Lite UDP Received bytes.
lsndsliteudprxbytesrate	<Double>	Read-only	Rate (/s) counter for lsntotdsliteudprxbytes
lsntotdsliteudptxpkts	<Double>	Read-only	Number of LSN DS-Lite UDP Transmitted packets.
lsndsliteudptxpktsrate	<Double>	Read-only	Rate (/s) counter for lsntotdsliteudptxpkts
lsntotdsliteudptxbytes	<Double>	Read-only	Number of LSN DS-Lite UDP Transmitted bytes.
lsndsliteudptxbytesrate	<Double>	Read-only	Rate (/s) counter for lsntotdsliteudptxbytes
lsntotdsliteudpdrppkts	<Double>	Read-only	Number of LSN DS-Lite UDP Dropped packets.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
lsndsliteudpdrppktsrate	<Double>	Read-only	Rate (/s) counter for lsntotdsliteudpdrppkts
lsncurdsliteudpsessions	<Double>	Read-only	Number of LSN DS-Lite UDP Current Sessions.
lsncurdsliteudpsessionsrate	<Double>	Read-only	Rate (/s) counter for lsncurdsliteudpsessions
lsntotdsliteicmprxpkts	<Double>	Read-only	Number of LSN DS-Lite ICMP Received packets.
lsndsliteicmprxpktsrate	<Double>	Read-only	Rate (/s) counter for lsntotdsliteicmprxpkts
lsntotdsliteicmprxbytes	<Double>	Read-only	Number of LSN DS-Lite ICMP Received bytes.
lsndsliteicmprxbytesrate	<Double>	Read-only	Rate (/s) counter for lsntotdsliteicmprxbytes
lsntotdsliteicmptxpkts	<Double>	Read-only	Number of LSN DS-Lite ICMP Transmitted packets.
lsndsliteicmptxpktsrate	<Double>	Read-only	Rate (/s) counter for lsntotdsliteicmptxpkts
lsntotdsliteicmptxbytes	<Double>	Read-only	Number of LSN DS-Lite ICMP Transmitted bytes.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
lsndsliteicmptxbytesrate	<Double>	Read-only	Rate (/s) counter for lsntotdsliteicmptxbytes
lsntotdsliteicmpdrppkts	<Double>	Read-only	Number of LSN DS-Lite ICMP Dropped packets.
lsndsliteicmpdrppktsrate	<Double>	Read-only	Rate (/s) counter for lsntotdsliteicmpdrppkts
lsncurdsliteicmpsessions	<Double>	Read-only	Number of LSN DS-Lite ICMP Current Sessions.
lsncurdsliteicmpsessionsrate	<Double>	Read-only	Rate (/s) counter for lsncurdsliteicmpsessions
lsncurdslitesessions	<Double>	Read-only	Current number of LSN DS-Lite sessions.
lsncurdslitesessionsrate	<Double>	Read-only	Rate (/s) counter for lsncurdslitesessions
lsndslitecursubscribers	<Double>	Read-only	Current number of LSN DS-Lite subscribers.
lsndslitecursubscribersrate	<Double>	Read-only	Rate (/s) counter for lsndslitecursubscribers

Operations

(click to see Properties)

- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/lsndslite **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/lsndslite? **args=detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get lsndslite resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/lsndslite? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lsndslite": [ {

"lsntotdsliteudprxpkts":<Double_value>,

"lsndslitetcpdrppktsrate":<Double_value>,

"lsncurdslitetcpsessions":<Double_value>,

"lsndsliteicmptxbytesrate":<Double_value>,

"lsntotdslitetcprxbytes":<Double_value>,

"lsntotdsliterxbytes":<Double_value>,

"lsndsliteudptxpktsrate":<Double_value>,

"lsntotdslitetxbytes":<Double_value>,

"lsntotdsliteicmprxbytes":<Double_value>,

"lsndsliteudprxpktsrate":<Double_value>,

"lsndsliteudprxbytesrate":<Double_value>,

"lsntotdsliteicmpdrppkts":<Double_value>,

"lsncurdsliteicmpsessions":<Double_value>,

"lsntotdsliteicmptxbytes":<Double_value>,

"lsndsliteudptxbytesrate":<Double_value>,
```

```
"lsntotdslitetcprxpkts":<Double_value>,

"lsndslitetcptxpktsrate":<Double_value>,

"lsndslitetcprxpktsrate":<Double_value>,

"lsntotdsliteicmprxpkts":<Double_value>,

"lsndsliteicmpdrppktsrate":<Double_value>,

"lsndslitetcprxbytesrate":<Double_value>,

"lsndsliteicmprxpktsrate":<Double_value>,

"lsncurdsliteudpsessions":<Double_value>,

"lsndslitetcptxbytesrate":<Double_value>,

"lsntotdsliteudprxbytes":<Double_value>,

"lsncurdslitetcpsessionsrate":<Double_value>,

"lsntotdsliteicmptxpkts":<Double_value>,

"lsndslitecursubscribers":<Double_value>,

"lsntotdslitetxpkts":<Double_value>,

"lsntotdsliterxpkts":<Double_value>,

"lsndsliteudpdrppktsrate":<Double_value>,

"lsndsliterxpktsrate":<Double_value>,

"lsndslitetxpktsrate":<Double_value>,

"lsntotdsliteudpdrppkts":<Double_value>,

"lsndsliteicmptxpktsrate":<Double_value>,

"lsntotdslitetcptxpkts":<Double_value>,

"lsncurdsliteicmpsessionsrate":<Double_value>,
```

```
"lsndslitecursubscribersrate":<Double_value>,

"lsntotdsliteudptxbytes":<Double_value>,

"lsndslitetxbytesrate":<Double_value>,

"lsntotdslitetcpdrppkts":<Double_value>,

"lsndsliterxbytesrate":<Double_value>,

"lsncurdsliteudpsessionsrate":<Double_value>,

"lsncurdslitesessionsrate":<Double_value>,

"lsndsliteicmprxbytesrate":<Double_value>,

"lsncurdslitesessions":<Double_value>,

"lsntotdsliteudptxpkts":<Double_value>,

"lsntotdslitetcptxbytes":<Double_value>

}]}
```

lsngroup

Statistics for LSN group resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
groupname	<String>	Read-write	Name of the LSN Group. Minimum length = 1 Maximum length = 127

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full
lsngrpcursessions	<Double>	Read-only	Number of Current Sessions for LSN group
lsngrpcursessionsrate	<Double>	Read-only	Rate (/s) counter for lsngrpcursessions
lsngrptottranslbytes	<Double>	Read-only	Number of Translated Bytes for LSN group
lsngrptranslbytesrate	<Double>	Read-only	Rate (/s) counter for lsngrptottranslbytes
lsngrptottranslpkts	<Double>	Read-only	Number of Translated Pkts for LSN group
lsngrptranslpktsrate	<Double>	Read-only	Rate (/s) counter for lsngrptottranslpkts
lsngrptottcptranslpkts	<Double>	Read-only	Number of TCP Translated Pkts for LSN group
lsngrptcptranslpktsrate	<Double>	Read-only	Rate (/s) counter for lsngrptottcptranslpkts
lsngrptottcptranslbytes	<Double>	Read-only	Number of TCP Translated Bytes for LSN group
lsngrptcptranslbytesrate	<Double>	Read-only	Rate (/s) counter for lsngrptottcptranslbytes

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
lsngrptottcpdrppkts	<Double>	Read-only	Number of TCP Dropped Pkts for LSN group
lsngrptcpdrppktsrate	<Double>	Read-only	Rate (/s) counter for lsngrptottcpdrppkts
lsngrpcurtcpsessions	<Double>	Read-only	Number of TCP Current Sessions for LSN group
lsngrpcurtcpsessions rate	<Double>	Read-only	Rate (/s) counter for lsngrpcurtcpsessions
lsngrptotudptranslpkt s	<Double>	Read-only	Number of UDP Translated Pkts for LSN group
lsngrpudptranslpktsr ate	<Double>	Read-only	Rate (/s) counter for lsngrptotudptranslpkt s
lsngrptotudptranslbyt es	<Double>	Read-only	Number of UDP Translated Bytes for LSN group
lsngrpudptranslbytes rate	<Double>	Read-only	Rate (/s) counter for lsngrptotudptranslbyt es
lsngrptotudpdrppkts	<Double>	Read-only	Number of UDP Dropped Pkts for LSN group
lsngrpudpdrppktsrate	<Double>	Read-only	Rate (/s) counter for lsngrptotudpdrppkts
lsngrpcurudpsession s	<Double>	Read-only	Number of UDP Current Sessions for LSN group

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
lsngrpcurudpsessionsrate	<Double>	Read-only	Rate (/s) counter for lsngrpcurudpsessions
lsngrptoticmptranslpkts	<Double>	Read-only	Number of ICMP Translated Pkts for LSN group
lsngrpicmptranslpktsrate	<Double>	Read-only	Rate (/s) counter for lsngrptoticmptranslpkts
lsngrptoticmptranslbytes	<Double>	Read-only	Number of ICMP Translated Bytes for LSN group
lsngrpicmptranslbytesrate	<Double>	Read-only	Rate (/s) counter for lsngrptoticmptranslbytes
lsngrptoticmpdrppkts	<Double>	Read-only	Number of ICMP Dropped Pkts for LSN group
lsngrpicmpdrppktsrate	<Double>	Read-only	Rate (/s) counter for lsngrptoticmpdrppkts
lsngrpcuricmpsessions	<Double>	Read-only	Number of ICMP Current Sessions for LSN group
lsngrpcuricmpsessionsrate	<Double>	Read-only	Rate (/s) counter for lsngrpcuricmpsessions
lsngrpcursubscribers	<Double>	Read-only	Number of ICMP Current Sessions for LSN group
lsngrpcursubscribersrate	<Double>	Read-only	Rate (/s) counter for lsngrpcursubscribers

Operations

(click to see Properties)

- GET (ALL)
- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/lsngroup **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/lsngroup? **args=groupname: <String_value> ,detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get lsngroup resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/lsngroup? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lsngroup": [ {

"groupname":<String_value>,

"lsngrpcurtcpsessions":<Double_value>,

"lsngrpicmptranslpktsrate":<Double_value>,

"lsngrpcuricmpsessions":<Double_value>,

"lsngrpudptranslpktsrate":<Double_value>,

"lsngrptcpdrppktsrate":<Double_value>,

"lsngrptottranslbytes":<Double_value>,

"lsngrpcurtcpsessionsrate":<Double_value>,

"lsngrpcursessions":<Double_value>,
```

```
"lsngrptcptranslbytesrate":<Double_value>,

"lsngrptoticmpdrppkts":<Double_value>,

"lsngrpcursubscribersrate":<Double_value>,

"lsngrpcuricmpsessionsrate":<Double_value>,

"lsngrpcurudpsessionsrate":<Double_value>,

"lsngrptoticmptranslbytes":<Double_value>,

"lsngrpcursubscribers":<Double_value>,

"lsngrpcurudpsessions":<Double_value>,

"lsngrptranslbytesrate":<Double_value>,

"lsngrpcursessionsrate":<Double_value>,

"lsngrpicmptranslbytesrate":<Double_value>,

"lsngrptottranslpkts":<Double_value>,

"lsngrptotudpdrppkts":<Double_value>,

"lsngrpudpdrppktsrate":<Double_value>,

"lsngrptcptranslpktsrate":<Double_value>,

"lsngrpudptranslbytesrate":<Double_value>,

"lsngrptottcptranslbytes":<Double_value>,

"lsngrptotudptranslpkts":<Double_value>,

"lsngrptoticmptranslpkts":<Double_value>,

"lsngrpicmpdrppktsrate":<Double_value>,

"lsngrptottcpdrppkts":<Double_value>,

"lsngrptranslpktsrate":<Double_value>,
```

```
"lsngrptotudptranslbytes":<Double_value>,

"lsngrptottcptranslpkts":<Double_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/stat/lsngroup/ groupname_value><String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lsngroup": [ {

"groupname":<String_value>,

"lsngrpcurtcpsessions":<Double_value>,

"lsngrpicmptranslpktsrate":<Double_value>,

"lsngrpcuricmpsessions":<Double_value>,

"lsngrpudptranslpktsrate":<Double_value>,

"lsngrptcpdrppktsrate":<Double_value>,

"lsngrptottranslbytes":<Double_value>,
```

```
"lsngrpcurtcpsessionsrate":<Double_value>,

"lsngrpcursessions":<Double_value>,

"lsngrptcptranslbytesrate":<Double_value>,

"lsngrptoticmpdrppkts":<Double_value>,

"lsngrpcursubscribersrate":<Double_value>,

"lsngrpcuricmpsessionsrate":<Double_value>,

"lsngrpcurudpsessionsrate":<Double_value>,

"lsngrptoticmptranslbytes":<Double_value>,

"lsngrpcursubscribers":<Double_value>,

"lsngrpcurudpsessions":<Double_value>,

"lsngrptranslbytesrate":<Double_value>,

"lsngrpcursessionsrate":<Double_value>,

"lsngrpicmptranslbytesrate":<Double_value>,

"lsngrptottranslpkts":<Double_value>,

"lsngrptotudpdrppkts":<Double_value>,

"lsngrpudpdrppktsrate":<Double_value>,

"lsngrptcptranslpktsrate":<Double_value>,

"lsngrpudptranslbytesrate":<Double_value>,

"lsngrptottcptranslbytes":<Double_value>,

"lsngrptotudptranslpkts":<Double_value>,

"lsngrptoticmptranslpkts":<Double_value>,

"lsngrpicmpdrppktsrate":<Double_value>,
```

```
"lsngrptottcpdrppkts":<Double_value>,

"lsngrptranslpktsrate":<Double_value>,

"lsngrptotudptranslbytes":<Double_value>,

"lsngrptottcptranslpkts":<Double_value>

}]}
```

lsnnat64

Read/write properties

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full
lsncurnat64sessions	<Double>	Read-only	Current number of LSN NAT64 sessions.
lsncurnat64sessionsrate	<Double>	Read-only	Rate (/s) counter for lsncurnat64sessions
lsnnat64cursubscribers	<Double>	Read-only	Current number of LSN NAT64 subscribers.
lsnnat64cursubscribersrate	<Double>	Read-only	Rate (/s) counter for lsnnat64cursubscribers
lsntotnat64rxpkts	<Double>	Read-only	Total number of LSN NAT64 rx pkts.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
lsnnat64rxpktsrate	<Double>	Read-only	Rate (/s) counter for lsntotnat64rxpkts
lsntotnat64rxbytes	<Double>	Read-only	Total number of LSN NAT64 rx bytes.
lsnnat64rxbytesrate	<Double>	Read-only	Rate (/s) counter for lsntotnat64rxbytes
lsntotnat64txpkts	<Double>	Read-only	Total number of LSN NAT64 tx pkts.
lsnnat64txpktsrate	<Double>	Read-only	Rate (/s) counter for lsntotnat64txpkts
lsntotnat64txbytes	<Double>	Read-only	Total number of LSN NAT64 tx bytes.
lsnnat64txbytesrate	<Double>	Read-only	Rate (/s) counter for lsntotnat64txbytes
lsncurnat64tcpsessions	<Double>	Read-only	Number of LSN NAT64 TCP Current Sessions.
lsncurnat64tcpsessionsrate	<Double>	Read-only	Rate (/s) counter for lsncurnat64tcpsessions
lsntotnat64tcprxpkts	<Double>	Read-only	Number of LSN NAT64 TCP Received packets.
lsnnat64tcprxpktsrate	<Double>	Read-only	Rate (/s) counter for lsntotnat64tcprxpkts
lsntotnat64tcprxbytes	<Double>	Read-only	Number of LSN NAT64 TCP Received bytes.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
lsnnat64tcprxbytesrate	<Double>	Read-only	Rate (/s) counter for lsntotnat64tcprxbytes
lsntotnat64tcptxpkts	<Double>	Read-only	Number of LSN NAT64 TCP Transmitted packets.
lsnnat64tcptxpktsrate	<Double>	Read-only	Rate (/s) counter for lsntotnat64tcptxpkts
lsntotnat64tcptxbytes	<Double>	Read-only	Number of LSN NAT64 TCP Transmitted bytes.
lsnnat64tcptxbytesrate	<Double>	Read-only	Rate (/s) counter for lsntotnat64tcptxbytes
lsntotnat64tcpdrppkts	<Double>	Read-only	Number of LSN NAT64 TCP Dropped packets.
lsnnat64tcpdrppktsrate	<Double>	Read-only	Rate (/s) counter for lsntotnat64tcpdrppkts
lsncurnat64udpsessions	<Double>	Read-only	Number of LSN NAT64 UDP Current Sessions.
lsncurnat64udpsessionsrate	<Double>	Read-only	Rate (/s) counter for lsncurnat64udpsessions
lsntotnat64udprxpkts	<Double>	Read-only	Number of LSN NAT64 UDP Received packets.
lsnnat64udprxpktsrate	<Double>	Read-only	Rate (/s) counter for lsntotnat64udprxpkts

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
lsntotnat64udprxbytes	<Double>	Read-only	Number of LSN NAT64 UDP Received bytes.
lsnnat64udprxbytesrate	<Double>	Read-only	Rate (/s) counter for lsntotnat64udprxbytes
lsntotnat64udptxpkts	<Double>	Read-only	Number of LSN NAT64 UDP Transmitted packets.
lsnnat64udptxpktsrate	<Double>	Read-only	Rate (/s) counter for lsntotnat64udptxpkts
lsntotnat64udptxbytes	<Double>	Read-only	Number of LSN NAT64 UDP Transmitted bytes.
lsnnat64udptxbytesrate	<Double>	Read-only	Rate (/s) counter for lsntotnat64udptxbytes
lsntotnat64udpdrppkts	<Double>	Read-only	Number of LSN NAT64 UDP Dropped packets.
lsnnat64udpdrppktsrate	<Double>	Read-only	Rate (/s) counter for lsntotnat64udpdrppkts
lsncurnat64icmpsessions	<Double>	Read-only	Number of LSN NAT64 ICMP Current Sessions.
lsncurnat64icmpsessionsrate	<Double>	Read-only	Rate (/s) counter for lsncurnat64icmpsessions

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
lsntotnat64icmprxpkts	<Double>	Read-only	Number of LSN NAT64 ICMP Received packets.
lsnnat64icmprxpktsrate	<Double>	Read-only	Rate (/s) counter for lsntotnat64icmprxpkts
lsntotnat64icmprxbytes	<Double>	Read-only	Number of LSN NAT64 ICMP Received bytes.
lsnnat64icmprxbytesrate	<Double>	Read-only	Rate (/s) counter for lsntotnat64icmprxbytes
lsntotnat64icmptxpkts	<Double>	Read-only	Number of LSN NAT64 ICMP Transmitted packets.
lsnnat64icmptxpktsrate	<Double>	Read-only	Rate (/s) counter for lsntotnat64icmptxpkts
lsntotnat64icmptxbytes	<Double>	Read-only	Number of LSN NAT64 ICMP Transmitted bytes.
lsnnat64icmptxbytesrate	<Double>	Read-only	Rate (/s) counter for lsntotnat64icmptxbytes
lsntotnat64icmpdrppkts	<Double>	Read-only	Number of LSN NAT64 ICMP Dropped packets.
lsnnat64icmpdrppktsrate	<Double>	Read-only	Rate (/s) counter for lsntotnat64icmpdrppkts

Operations

(click to see Properties)

- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/lsnnat64 **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/lsnnat64? **args=detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get lsnnat64 resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/lsnnat64? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lsnnat64": [ {

"lsnnat64udprxbytesrate":<Double_value>,

"lsnnat64tcptxpktsrate":<Double_value>,

"lsnnat64tcptxbytesrate":<Double_value>,

"lsnnat64udprxpktsrate":<Double_value>,

"lsntotnat64tcprxbytes":<Double_value>,

"lsntotnat64tcptxbytes":<Double_value>,

"lsnnat64txbytesrate":<Double_value>,

"lsnnat64cursubscribersrate":<Double_value>,

"lsnnat64rxpktsrate":<Double_value>,

"lsnnat64udpdrppktsrate":<Double_value>,

"lsnnat64icmprxbytesrate":<Double_value>,
```

```
"lsncurnat64icmpsessions":<Double_value>,

"lsnnat64rxbytesrate":<Double_value>,

"lsntotnat64icmprxbytes":<Double_value>,

"lsnnat64icmptxbytesrate":<Double_value>,

"lsncurnat64icmpsessionsrate":<Double_value>,

"lsnnat64icmptxpktsrate":<Double_value>,

"lsnnat64txpktsrate":<Double_value>,

"lsnnat64icmprxpktsrate":<Double_value>,

"lsncurnat64sessions":<Double_value>,

"lsntotnat64txbytes":<Double_value>,

"lsncurnat64tcpsessionsrate":<Double_value>,

"lsnnat64cursubscribers":<Double_value>,

"lsncurnat64udpsessionsrate":<Double_value>,

"lsnnat64icmpdrppktsrate":<Double_value>,

"lsntotnat64icmprxpkts":<Double_value>,

"lsntotnat64udprxbytes":<Double_value>,

"lsntotnat64udptxbytes":<Double_value>,

"lsntotnat64rxpkts":<Double_value>,

"lsncurnat64udpsessions":<Double_value>,

"lsncurnat64sessionsrate":<Double_value>,

"lsntotnat64txpkts":<Double_value>,

"lsntotnat64icmptxpkts":<Double_value>,
```

```
"lsntotnat64udptxpkts":<Double_value>,

"lsntotnat64udprxpkts":<Double_value>,

"lsntotnat64udpdrppkts":<Double_value>,

"lsntotnat64rxbytes":<Double_value>,

"lsntotnat64icmptxbytes":<Double_value>,

"lsntotnat64tcptxpkts":<Double_value>,

"lsntotnat64tcprxpkts":<Double_value>,

"lsntotnat64tcpdrppkts":<Double_value>,

"lsnnat64udptxbytesrate":<Double_value>,

"lsnnat64tcprxpktsrate":<Double_value>,

"lsnnat64tcprxbytesrate":<Double_value>,

"lsnnat64udptxpktsrate":<Double_value>,

"lsntotnat64icmpdrppkts":<Double_value>,

"lsncurnat64tcpsessions":<Double_value>,

"lsnnat64tcpdrppktsrate":<Double_value>

}]}
```

lsnpool

Statistics for LSN pool resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
poolname	<String>	Read-write	Name of the LSN Pool. Minimum length = 1 Maximum length = 127
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full
lsnpoolotherportusagepercen	<Double>	Read-only	Other protocols ports usage percentage in this pool.
lsnpooltcpportusagepercen	<Double>	Read-only	TCP ports usage percentage in this pool.
lsnpoolcurportalloctcp	<Double>	Read-only	Current port allocation for tcp in this pool.
lsnpoolcurportalloctcprate	<Double>	Read-only	Rate (/s) counter for lsnpoolcurportalloctcp
lsnpoolcurportallocother	<Double>	Read-only	Current port allocation for other protocols in this pool.
lsnpoolcurportallocotherrate	<Double>	Read-only	Rate (/s) counter for lsnpoolcurportallocother
lsnpooltotips	<Double>	Read-only	Total IPs in this pool.

Operations

(click to see Properties)

- GET (ALL)
- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/lsnpool **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/lsnpool? **args=poolname: <String_value> ,detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get lsnpool resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/lsnpool? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lsnpool": [ {

"poolname":<String_value>,

"lsnpoolcurportallocotherrate":<Double_value>,

"lsnpoolcurportallocother":<Double_value>,

"lsnpooltcpportusagepercen":<Double_value>,

"lsnpoolcurportalloctcp":<Double_value>,

"lsnpoolcurportalloctcprate":<Double_value>,

"lsnpooltotips":<Double_value>,

"lsnpoolotherportusagepercen":<Double_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/stat/lsnpool/ poolname_value><String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lsnpool": [ {

"poolname":<String_value>,

"lsnpoolcurportallocotherrate":<Double_value>,

"lsnpoolcurportallocother":<Double_value>,

"lsnpooltcpportusagepercen":<Double_value>,

"lsnpoolcurportalloctcp":<Double_value>,

"lsnpoolcurportalloctcprate":<Double_value>,

"lsnpooltotips":<Double_value>,

"lsnpoolotherportusagepercen":<Double_value>

}]}
```

network

Network

Networking commands.

NAME	DESCRIPTION
Interface	Statistics for interface resource.
bridge	Statistics for bridge resource.
inat	Statistics for inbound nat resource.
inatsession	Statistics for stateful INAT resource.
mapbmr	Statistics for MAP-T Basic Mapping rule resource.
mapdomain	Statistics for MAP-T Map Domain resource.
nat64	Statistics for nat64 config resource.
rnat	Statistics for RNAT configured route resource.
rnat6	Statistics for IPv6 RNAT configured route resource.
rnatip	Statistics for RNAT ipaddress resource.
tunnelip	Statistics for TUNNEL Remote ipaddress resource.
tunnelip6	Statistics for TUNNEL Remote ip6address resource.
vlan	Statistics for "VLAN" resource.

NAME	DESCRIPTION
vxlan	Statistics for "VXLAN" resource.

Interface

Statistics for interface resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
id	<String>	Read-write	Interface number, in C/U format, where C can take one of the following values: * 0 - Indicates a management interface. * 1 - Indicates a 1 Gbps port. * 10 - Indicates a 10 Gbps port. * LA - Indicates a link aggregation port. * LO - Indicates a loop back port. U is a unique integer for representing an interface in a particular port group.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full
curintfstate	<String>	Read-only	Current state of the specified interface. The interface state set to UP only if the link state is UP and administrative state is ENABLED .
curlinkuptime	<String>	Read-only	Duration for which the link is UP. This statistic is reset when the state changes to DOWN.
curlinkdowntime	<String>	Read-only	Duration for which the link is DOWN. This statistic is reset when the state changes to UP.
totrxbytes	<Double>	Read-only	Number of bytes received by an interface since the Citrix ADC was started or the interface statistics were cleared.
rxbytesrate	<Double>	Read-only	Rate (/s) counter for totrxbytes
tottxbytes	<Double>	Read-only	Number of bytes transmitted by an interface since the Citrix ADC was started or the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			interface statistics were cleared.
txbytesrate	<Double>	Read-only	Rate (/s) counter for tottxbytes
totrxpkts	<Double>	Read-only	Number of packets received by an interface since the Citrix ADC was started or the interface statistics were cleared.
rxpktsrate	<Double>	Read-only	Rate (/s) counter for totrxpkts
tottxpkts	<Double>	Read-only	Number of packets transmitted by an interface since the Citrix ADC was started or the interface statistics were cleared.
txpktsrate	<Double>	Read-only	Rate (/s) counter for tottxpkts
jumbopktsreceived	<Double>	Read-only	Number of Jumbo Packets received on this interface.
jumbopktsreceivedrate	<Double>	Read-only	Rate (/s) counter for jumbopktsreceived
jumbopktstransmitted	<Double>	Read-only	Number of Jumbo packets transmitted on this interface by upper layer, with TSO enabled actual

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			trasmission size could be non Jumbo.
jumbopktstransmitted rate	<Double>	Read-only	Rate (/s) counter for jumbopktstransmitted
trunkpktsreceived	<Double>	Read-only	Number of Tagged Packets received on this Trunk interface through Allowed VLan List.
trunkpktsreceivedrate	<Double>	Read-only	Rate (/s) counter for trunkpktsreceived
trunkpktstransmitted	<Double>	Read-only	Number of Tagged Packets transmitted on this Trunk interface through Allowed VLan List.
trunkpktstransmittedrate	<Double>	Read-only	Rate (/s) counter for trunkpktstransmitted
nictotmulticastpkts	<Double>	Read-only	Number of multicast packets received by the specified interface since the Citrix ADC was started or the interface statistics were cleared.
nicmulticastpktsrate	<Double>	Read-only	Rate (/s) counter for nictotmulticastpkts
totnetscalerpkts	<Double>	Read-only	Number of packets, destined to the Citrix ADC, received by an interface since the Citrix ADC was

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			started or the interface statistics were cleared. The packets destined to Citrix ADC are those that have the same MAC address as that of an interface or a VMAC address owned by the Citrix ADC.
netscalerpktsrate	<Double>	Read-only	Rate (/s) counter for totnetscalerpkts
rxlacpdu	<Double>	Read-only	Number of Link Aggregation Control Protocol Data Units(LACPDUs) received by the specified interface since the Citrix ADC was started or the interface statistics were cleared.
rxlacpdurate	<Double>	Read-only	Rate (/s) counter for rxlacpdu
txlacpdu	<Double>	Read-only	Number of Link Aggregation Control Protocol Data Units(LACPDUs) transmitted by the specified interface since the Citrix ADC was started or the interface statistics were cleared.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
txlacpdurate	<Double>	Read-only	Rate (/s) counter for txlacpdu
errpktrx	<Double>	Read-only	Number of inbound packets dropped by the hardware on a specified interface once the Citrix ADC starts or the interface statistics are cleared. This happens due to following reasons: 1) The hardware receives packets at a rate higher rate than that at which the software is processing packets. In this case, the hardware FIFO overruns and starts dropping the packets . 2) The specified interface fails to receive inbound packets from the appliance because of insufficient memory. 3) The specified interface receives packets with CRC errors (Alignment or Frame Check Sequence). 4) The specified interface receives overly long packets. 5) The specified interface receives packets with alignment

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			errors. 6) The software does less buffering because it is running out of available memory. When hardware detects that there is no space into which to push newly arrived packets, it starts dropping them. 7) The specified interface receives packets with Frame Check Sequence (FCS) errors. 8) The specified interface receives packets smaller than 64 bytes. 9) The specified interface discards error-free inbound packets because of insufficient resources. For example: NIC buffers. 10) Packets are missed because of collision detection, link lost, physical decoding error, or MAC abort.
errpktrxrate	<Double>	Read-only	Rate (/s) counter for errpktrx
errpkttx	<Double>	Read-only	Number of outbound packets dropped by the hardware on a specified interface

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			since the Citrix ADC was started or the interface statistics were cleared. This could happen due to length (undersize or oversize) errors and lack of resources. This statistic is available only for: (1) Loop back interface (LO) of all platforms. (2) All data ports on the Citrix ADC 12000 platform. (3) Management ports on the MPX 15000 and 17000 platforms.
errpkttxrate	<Double>	Read-only	Rate (/s) counter for errpkttx
errifindiscards	<Double>	Read-only	Number of error-free inbound packets discarded by the specified interface due to a lack of resources, for example, insufficient receive buffers.
errifindiscardsrate	<Double>	Read-only	Rate (/s) counter for errifindiscards
nicerrifoutdiscards	<Double>	Read-only	Number of error-free outbound packets discarded by the specified interface due to a lack of resources. This statistic is not

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			available on: (1) 10G ports of Citrix ADC MPX 12500/12500/15500-10G platforms. (2) 10G data ports on Citrix ADC MPX 17500/19500/21500 platforms.
nicerrifoutdiscardsrate	<Double>	Read-only	Rate (/s) counter for nicerrifoutdiscards
errdroppedrxpkts	<Double>	Read-only	Number of inbound packets dropped by the specified interface. Commonly dropped packets are multicast frames, spanning tree BPDUs, packets destined to a MAC not owned by the Citrix ADC when L2 mode is disabled, or packets tagged for a VLAN that is not bound to the interface. This statistic will increment in most healthy networks at a steady rate regardless of traffic load. If a sharp spike in dropped packets occurs, it generally indicates an issue with connected L2 switches, such as a forwarding database

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			overflow resulting in packets being broadcast on all ports.
errdroppedrxpktsrate	<Double>	Read-only	Rate (/s) counter for errdroppedrxpkts
errdroppedtxpkts	<Double>	Read-only	Number of packets dropped in transmission by the specified interface due to one of the following reasons. (1) VLAN mismatch. (2) Oversized packets. (3) Interface congestion. (4) Loopback packets sent on non loop back interface.
errdroppedtxpktsrate	<Double>	Read-only	Rate (/s) counter for errdroppedtxpkts
errlinkhangs	<Double>	Read-only	Number of times the specified interface detected hangs in the transmit and receive paths since the Citrix ADC was started or the interface statistics were cleared.
nicstsstalls	<Double>	Read-only	Number of times the status updates for a specified interface were stalled since the Citrix ADC was started or the interface statistics

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			were cleared. A status stall is detected when the status of the interface is not updated by the NIC hardware within 0.8 seconds of the last update.
nictxstalls	<Double>	Read-only	Number of times the interface stalled, when transmitting packets, since the Citrix ADC was started or the interface statistics were cleared. Transmit (Tx) stalls are detected when a packet posted for transmission is not transmitted in 4 seconds.
nicrxstalls	<Double>	Read-only	Number of times the interface stalled, when receiving packets, since the Citrix ADC was started or the interface statistics were cleared. Receive (Rx) stalls are detected when the following conditions are met: (1)The link is up for more than 10 minutes. (2)Packets are transmitted, but

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			no packets is received for 16 seconds.
nicerrdisables	<Double>	Read-only	Number of times the specified interface is disabled by the Citrix ADC, due to continuous Receive (Rx) or Transmit (Tx) stalls, since the Citrix ADC was started or the interface statistics were cleared. The Citrix ADC disables an interface when one of the following conditions is met: (1) Three consecutive transmit stalls occurs with at most gap of 10 seconds between any two stalls. (2) Three consecutive receive stalls occurs with at most gap of 120 seconds between any two stalls.
linkreinits	<Double>	Read-only	Number of times the link has been re-initialized. A re-initialization occurs due to link state change, configuration parameter change, or administrative reset operation.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
totmacmoved	<Double>	Read-only	Number of MAC moves between ports. If a high rate of MAC moves is observed, it is likely that there is a bridge loop between two interfaces.
macmovedrate	<Double>	Read-only	Rate (/s) counter for totmacmoved
errnicmuted	<Double>	Read-only	Number of times the specified interface stopped transmitting and receiving packets due to MAC moves between ports.
rxcrcerrors	<Double>	Read-only	Number of packets received with the wrong checksum by the specified interface since the Citrix ADC was started or the interface statistics were cleared. This indicates the number of Jabber frames received instead of CRC errors on the 10G data ports of Citrix ADC 12000-10G platform and the data ports of Citrix ADC MPX 15000 and 17000 platforms.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
rxcrcerrorsrate	<Double>	Read-only	Rate (/s) counter for rxcrcerrors
interfacealias	<String>	Read-only	Alias Name for the Interface
curlinkstate	<String>	Read-only	The current state of the link associated with the interface. For logical interfaces (LA), the state of the link is dependent on the state of the slave interfaces. For the link to be UP at least one of the slave interfaces needs to be UP.

Operations

(click to see Properties)

- GET (ALL)
- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.
- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/Interface **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/Interface? **args=id: <String_value> ,detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get Interface resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/Interface? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "Interface": [ {

"id":<String_value>,

"curlinkdowntime":<String_value>,

"txpktsrate":<Double_value>,

"nicerrifoutdiscardsrate":<Double_value>,

"trunkpktstransmittedrate":<Double_value>,

"rxcrcerrorsrate":<Double_value>,

"nictxstalls":<Double_value>,

"trunkpktsreceived":<Double_value>,

"totrxpkts":<Double_value>,

"errpktrxrate":<Double_value>,

"errdroppedtxpkts":<Double_value>,

"errdroppedtxpktsrate":<Double_value>,

"trunkpktstransmitted":<Double_value>,

"interfacealias":<String_value>,

"nicerrdisables":<Double_value>,

"trunkpktsreceivedrate":<Double_value>,

"netscalerpktsrate":<Double_value>,

"rxpktsrate":<Double_value>,

"errdroppedrxpktsrate":<Double_value>,

"totnetscalerpkts":<Double_value>,

"errlinkhangs":<Double_value>,
```

```
"errdroppedrxpkts":<Double_value>,

"macmovedrate":<Double_value>,

"nictotmulticastpkts":<Double_value>,

"tottxpkts":<Double_value>,

"errifindiscards":<Double_value>,

"nicrxstalls":<Double_value>,

"errpktrx":<Double_value>,

"curlinkuptime":<String_value>,

"rxlacpdurate":<Double_value>,

"txlacpdu":<Double_value>,

"tottxbytes":<Double_value>,

"jumbopktstransmittedrate":<Double_value>,

"linkreinits":<Double_value>,

"jumbopktsreceived":<Double_value>,

"errpkttx":<Double_value>,

"curlinkstate":<String_value>,

"jumbopktstransmitted":<Double_value>,

"nicstsstalls":<Double_value>,

"rxbytesrate":<Double_value>,

"totmacmoved":<Double_value>,

"nicmulticastpktsrate":<Double_value>,

"jumbopktsreceivedrate":<Double_value>,
```

```
"rxlacpdu":<Double_value>,

"txlacpdurate":<Double_value>,

"errifindiscardsrate":<Double_value>,

"errpkttxrate":<Double_value>,

"nicerrifoutdiscards":<Double_value>,

"errnicmuted":<Double_value>,

"curintfstate":<String_value>,

"totrxbytes":<Double_value>,

"rxcrcerrors":<Double_value>,

"txbytesrate":<Double_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/stat/Interface/ id_value><String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "Interface": [ {

"id":<String_value>,

"curlinkdowntime":<String_value>,

"txpktsrate":<Double_value>,

"nicerrifoutdiscardsrate":<Double_value>,

"trunkpktstransmittedrate":<Double_value>,

"rxcrcerrorsrate":<Double_value>,

"nictxstalls":<Double_value>,

"trunkpktsreceived":<Double_value>,

"totrxpkts":<Double_value>,

"errpktrxrate":<Double_value>,

"errdroppedtxpkts":<Double_value>,

"errdroppedtxpktsrate":<Double_value>,

"trunkpktstransmitted":<Double_value>,

"interfacealias":<String_value>,

"nicerrdisables":<Double_value>,

"trunkpktsreceivedrate":<Double_value>,

"netscalerpktsrate":<Double_value>,

"rxpktsrate":<Double_value>,

"errdroppedrxpktsrate":<Double_value>,

"totnetscalerpkts":<Double_value>,

"errlinkhangs":<Double_value>,
```

```
"errdroppedrxpkts":<Double_value>,

"macmovedrate":<Double_value>,

"nictotmulticastpkts":<Double_value>,

"tottxpkts":<Double_value>,

"errifindiscards":<Double_value>,

"nicrxstalls":<Double_value>,

"errpktrx":<Double_value>,

"curlinkuptime":<String_value>,

"rxlacpdurate":<Double_value>,

"txlacpdu":<Double_value>,

"tottxbytes":<Double_value>,

"jumbopktstransmittedrate":<Double_value>,

"linkreinits":<Double_value>,

"jumbopktsreceived":<Double_value>,

"errpkttx":<Double_value>,

"curlinkstate":<String_value>,

"jumbopktstransmitted":<Double_value>,

"nicstsstalls":<Double_value>,

"rxbytesrate":<Double_value>,

"totmacmoved":<Double_value>,

"nicmulticastpktsrate":<Double_value>,

"jumbopktsreceivedrate":<Double_value>,
```

```
"rxlacpdu":<Double_value>,

"txlacpdurate":<Double_value>,

"errifindiscardsrate":<Double_value>,

"errpkttxrate":<Double_value>,

"nicerrifoutdiscards":<Double_value>,

"errnicmuted":<Double_value>,

"curintfstate":<String_value>,

"totrxbytes":<Double_value>,

"rxcrcerrors":<Double_value>,

"txbytesrate":<Double_value>

}]}
```

bridge

Statistics for bridge resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full
tcptotbdgmacmoved	<Double>	Read-only	The number of times bridging registered MAC moved

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
tcpbdgmacmovedrate	<Double>	Read-only	Rate (/s) counter for tcptotbdgmacmoved
tcptotbdgcollisions	<Double>	Read-only	The number of bridging table collisions
tcpbdgcollisionsrate	<Double>	Read-only	Rate (/s) counter for tcptotbdgcollisions
tcperrbdgmuted	<Double>	Read-only	The number of bridging related interface mutes
tcperrbdgmutedrate	<Double>	Read-only	Rate (/s) counter for tcperrbdgmuted
totbdgpkts	<Double>	Read-only	The total number of bridged packets
bdgpktsrate	<Double>	Read-only	Rate (/s) counter for totbdgpkts
totbdgmbits	<Double>	Read-only	The total number of bridged Mbits
bdgmbitsrate	<Double>	Read-only	Rate (/s) counter for totbdgmbits

Operations

(click to see Properties)

- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/bridge **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/bridge? **args=detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get bridge resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/bridge? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "bridge": [ {

"bdgmbitsrate":<Double_value>,

"tcptotbdgcollisions":<Double_value>,

"bdgpktsrate":<Double_value>,

"tcptotbdgmacmoved":<Double_value>,

"tcperrbdgmutedrate":<Double_value>,

"tcpbdgcollisionsrate":<Double_value>,

"tcperrbdgmuted":<Double_value>,

"totbdgmbits":<Double_value>,

"tcpbdgmacmovedrate":<Double_value>,

"totbdgpkts":<Double_value>

}]}
```

inat

Statistics for inbound nat resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	The INAT. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full
nat46tottcp46	<Double>	Read-only	Total TCP packets translated (V4->v6).
nat46tcp46rate	<Double>	Read-only	Rate (/s) counter for nat46tottcp46
nat46totudp46	<Double>	Read-only	Total UDP packets translated (V4->v6).
nat46udp46rate	<Double>	Read-only	Rate (/s) counter for nat46totudp46
nat46toticmp46	<Double>	Read-only	Total ICMP packets translated (V4->v6).
nat46icmp46rate	<Double>	Read-only	Rate (/s) counter for nat46toticmp46
nat46totdrop46	<Double>	Read-only	Total IPV4 packets dropped.
nat46drop46rate	<Double>	Read-only	Rate (/s) counter for nat46totdrop46
nat46tottcp64	<Double>	Read-only	Total TCP packets translated (V6->v4).
nat46tcp64rate	<Double>	Read-only	Rate (/s) counter for nat46tottcp64
nat46totudp64	<Double>	Read-only	Total UDP packets translated (V6->v4).
nat46udp64rate	<Double>	Read-only	Rate (/s) counter for nat46totudp64

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
nat46toticmp64	<Double>	Read-only	Total ICMP packets translated (V6->v4).
nat46icmp64rate	<Double>	Read-only	Rate (/s) counter for nat46toticmp64
nat46totdrop64	<Double>	Read-only	Total IPV6 packets dropped.
nat46drop64rate	<Double>	Read-only	Rate (/s) counter for nat46totdrop64
inatnat46tcp46	<Double>	Read-only	TCP packets translated (V4->v6).
inatnat46tcp46rate	<Double>	Read-only	Rate (/s) counter for inatnat46tcp46
inatnat46udp46	<Double>	Read-only	UDP packets translated (V4->v6).
inatnat46udp46rate	<Double>	Read-only	Rate (/s) counter for inatnat46udp46
inatnat46icmp46	<Double>	Read-only	ICMP packets translated (V4->v6).
inatnat46icmp46rate	<Double>	Read-only	Rate (/s) counter for inatnat46icmp46
inatnat46drop46	<Double>	Read-only	IPV4 packets dropped.
inatnat46drop46rate	<Double>	Read-only	Rate (/s) counter for inatnat46drop46
inatnat46tcp64	<Double>	Read-only	TCP packets translated (V6->v4).
inatnat46tcp64rate	<Double>	Read-only	Rate (/s) counter for inatnat46tcp64

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
inatnat46udp64	<Double>	Read-only	UDP packets translated (V6->v4).
inatnat46udp64rate	<Double>	Read-only	Rate (/s) counter for inatnat46udp64
inatnat46icmp64	<Double>	Read-only	ICMP packets translated (V6->v4).
inatnat46icmp64rate	<Double>	Read-only	Rate (/s) counter for inatnat46icmp64
inatnat46drop64	<Double>	Read-only	IPV6 packets dropped.
inatnat46drop64rate	<Double>	Read-only	Rate (/s) counter for inatnat46drop64

Operations

(click to see Properties)

- GET (ALL)
- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.
- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/inat **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/inat? **args=name: <String_value> ,detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get inat resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/inat? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "inat": [ {

"name":<String_value>,

"nat46tcp46rate":<Double_value>,

"nat46udp64rate":<Double_value>,

"nat46tottcp64":<Double_value>,

"inatnat46udp64rate":<Double_value>,

"inatnat46tcp64":<Double_value>,

"nat46toticmp64":<Double_value>,

"nat46totudp46":<Double_value>,

"inatnat46drop64":<Double_value>,

"inatnat46icmp64rate":<Double_value>,

"nat46drop46rate":<Double_value>,

"inatnat46drop46":<Double_value>,

"inatnat46icmp46rate":<Double_value>,

"nat46icmp64rate":<Double_value>,

"nat46totdrop64":<Double_value>,

"inatnat46udp64":<Double_value>,

"inatnat46tcp64rate":<Double_value>,

"inatnat46udp46rate":<Double_value>,

"inatnat46tcp46":<Double_value>,

"nat46drop64rate":<Double_value>,

"inatnat46icmp64":<Double_value>,
```

```
"inatnat46drop64rate":<Double_value>,

"nat46tcp64rate":<Double_value>,

"nat46udp46rate":<Double_value>,

"nat46toticmp46":<Double_value>,

"nat46tottcp46":<Double_value>,

"nat46icmp46rate":<Double_value>,

"inatnat46udp46":<Double_value>,

"inatnat46tcp46rate":<Double_value>,

"nat46totdrop46":<Double_value>,

"nat46totudp64":<Double_value>,

"inatnat46icmp46":<Double_value>,

"inatnat46drop46rate":<Double_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/stat/inat/ name_value><String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "inat": [ {

"name":<String_value>,

"nat46tcp46rate":<Double_value>,

"nat46udp64rate":<Double_value>,

"nat46tottcp64":<Double_value>,

"inatnat46udp64rate":<Double_value>,

"inatnat46tcp64":<Double_value>,

"nat46toticmp64":<Double_value>,

"nat46totudp46":<Double_value>,

"inatnat46drop64":<Double_value>,

"inatnat46icmp64rate":<Double_value>,

"nat46drop46rate":<Double_value>,

"inatnat46drop46":<Double_value>,

"inatnat46icmp46rate":<Double_value>,

"nat46icmp64rate":<Double_value>,

"nat46totdrop64":<Double_value>,

"inatnat46udp64":<Double_value>,

"inatnat46tcp64rate":<Double_value>,

"inatnat46udp46rate":<Double_value>,

"inatnat46tcp46":<Double_value>,
```

```
"nat46drop64rate":<Double_value>,

"inatnat46icmp64":<Double_value>,

"inatnat46drop64rate":<Double_value>,

"nat46tcp64rate":<Double_value>,

"nat46udp46rate":<Double_value>,

"nat46toticmp46":<Double_value>,

"nat46tottcp46":<Double_value>,

"nat46icmp46rate":<Double_value>,

"inatnat46udp46":<Double_value>,

"inatnat46tcp46rate":<Double_value>,

"nat46totdrop46":<Double_value>,

"nat46totudp64":<Double_value>,

"inatnat46icmp46":<Double_value>,

"inatnat46drop46rate":<Double_value>

}]}
```

inatsession

Statistics for stateful INAT resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	INAT name. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full
globalinathits	<Double>	Read-only	Total INAT Session hits
globalinathitsrate	<Double>	Read-only	Rate (/s) counter for globalinathits
globalinatcursessions	<Double>	Read-only	Total INAT current sessions
globalinatcursessionsrate	<Double>	Read-only	Rate (/s) counter for globalinatcursessions
globalinatreceivebytes	<Double>	Read-only	Total INAT Received Bytes
globalinatreceivebytesrate	<Double>	Read-only	Rate (/s) counter for globalinatreceivebytes
globalinattotsentbytes	<Double>	Read-only	Total INAT Sent Bytes
globalinatsentbytesrate	<Double>	Read-only	Rate (/s) counter for globalinattotsentbytes
globalinatpktreceived	<Double>	Read-only	Total INAT Packets Received
globalinatpktreceivedrate	<Double>	Read-only	Rate (/s) counter for globalinatpktreceived
globalinatpktsent	<Double>	Read-only	Total INAT Packets Sent

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
globalinatpktsentrate	<Double>	Read-only	Rate (/s) counter for globalinatpktsent
inattothits	<Double>	Read-only	INAT total sessions
inathitsrate	<Double>	Read-only	Rate (/s) counter for inattothits
inatcursessions	<Double>	Read-only	INAT current sessions
inatcursessionsrate	<Double>	Read-only	Rate (/s) counter for inatcursessions
inattotreceivebytes	<Double>	Read-only	INAT total Received Bytes
inatreceivebytesrate	<Double>	Read-only	Rate (/s) counter for inattotreceivebytes
inattotsentbytes	<Double>	Read-only	INAT total Sent Bytes
inatsentbytesrate	<Double>	Read-only	Rate (/s) counter for inattotsentbytes
inattotpktreceived	<Double>	Read-only	INAT total Packets Received
inatpktreceivedrate	<Double>	Read-only	Rate (/s) counter for inattotpktreceived
inattotpktsent	<Double>	Read-only	INAT total Packets Sent
inatpktsentrate	<Double>	Read-only	Rate (/s) counter for inattotpktsent

Operations

(click to see Properties)

- GET (ALL)
- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/inatsession **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/inatsession? **args=name: <String_value> ,detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get inatsession resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/inatsession? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "inatsession": [ {

"name":<String_value>,

"globalinathitsrate":<Double_value>,

"inatsentbytesrate":<Double_value>,

"inatpktreceivedrate":<Double_value>,

"inattothits":<Double_value>,

"globalinattotsentbytes":<Double_value>,

"inattotpktsent":<Double_value>,

"inatcursessions":<Double_value>,

"inattotsentbytes":<Double_value>,

"globalinatcursessionsrate":<Double_value>,

"globalinatpktreceivedrate":<Double_value>,

"globalinathits":<Double_value>,
```

```
"inattotreceivebytes":<Double_value>,

"globalinatpktsent":<Double_value>,

"globalinatreceivebytes":<Double_value>,

"inattotpktreceived":<Double_value>,

"inathitsrate":<Double_value>,

"globalinatcursessions":<Double_value>,

"inatreceivebytesrate":<Double_value>,

"inatpktsentrate":<Double_value>,

"globalinatsentbytesrate":<Double_value>,

"globalinatpktsentrate":<Double_value>,

"inatcursessionsrate":<Double_value>,

"globalinatreceivebytesrate":<Double_value>,

"globalinatpktreceived":<Double_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/stat/inatsession/ name_value><String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "inatsession": [ {

"name":<String_value>,

"globalinathitsrate":<Double_value>,

"inatsentbytesrate":<Double_value>,

"inatpktreceivedrate":<Double_value>,

"inattothits":<Double_value>,

"globalinattotsentbytes":<Double_value>,

"inattotpktsent":<Double_value>,

"inatcursessions":<Double_value>,

"inattotsentbytes":<Double_value>,

"globalinatcursessionsrate":<Double_value>,

"globalinatpktreceivedrate":<Double_value>,

"globalinathits":<Double_value>,

"inattotreceivebytes":<Double_value>,

"globalinatpktsent":<Double_value>,

"globalinatreceivebytes":<Double_value>,

"inattotpktreceived":<Double_value>,
```

```
"inathitsrate":<Double_value>,

"globalinatcursessions":<Double_value>,

"inatreceivebytesrate":<Double_value>,

"inatpktsentrate":<Double_value>,

"globalinatsentbytesrate":<Double_value>,

"globalinatpktsentrate":<Double_value>,

"inatcursessionsrate":<Double_value>,

"globalinatreceivebytesrate":<Double_value>,

"globalinatpktreceived":<Double_value>

}]}
```

mapbmr

Statistics for MAP-T Basic Mapping rule resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Basic Mapping Rule name. Minimum length = 1 Maximum length = 127
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
bmrtotv6rxpkts	<Double>	Read-only	Total number of MAP-T BMR V6 Recieved packets.
bmrv6rxpktsrate	<Double>	Read-only	Rate (/s) counter for bmrtotv6rxpkts
bmrtotv6txpkts	<Double>	Read-only	Total number of MAP-T BMR V6 Transmitted packets.
bmrv6txpktsrate	<Double>	Read-only	Rate (/s) counter for bmrtotv6txpkts
bmrtotv4rxpkts	<Double>	Read-only	Total number of MAP-T BMR V4 Recieved packets.
bmrv4rxpktsrate	<Double>	Read-only	Rate (/s) counter for bmrtotv4rxpkts
bmrtotv4txpkts	<Double>	Read-only	Total number of MAP-T BMR V4 Transmitted packets.
bmrv4txpktsrate	<Double>	Read-only	Rate (/s) counter for bmrtotv4txpkts
bmrtotv6rxpktstcp	<Double>	Read-only	Total number of MAP-T BMR V6 TCP Recieved packets.
bmrv6rxpktstcprate	<Double>	Read-only	Rate (/s) counter for bmrtotv6rxpktstcp
bmrtotv6txpktstcp	<Double>	Read-only	Total number of MAP-T BMR V6 TCP Transmitted packets.
bmrv6txpktstcprate	<Double>	Read-only	Rate (/s) counter for bmrtotv6txpktstcp

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
bmrtotv4rxpktstcp	<Double>	Read-only	Total number of MAP-T BMR V4 TCP Recieved packets.
bmrv4rxpktstcprate	<Double>	Read-only	Rate (/s) counter for bmrtotv4rxpktstcp
bmrtotv4txpktstcp	<Double>	Read-only	Total number of MAP-T BMR V4 TCP Transmitted packets.
bmrv4txpktstcprate	<Double>	Read-only	Rate (/s) counter for bmrtotv4txpktstcp
bmrtotv6rxpktsudp	<Double>	Read-only	Total number of MAP-T BMR V6 UDP Recieved packets.
bmrv6rxpktsudprate	<Double>	Read-only	Rate (/s) counter for bmrtotv6rxpktsudp
bmrtotv6txpktsudp	<Double>	Read-only	Total number of MAP-T BMR V6 UDP Transmitted packets.
bmrv6txpktsudprate	<Double>	Read-only	Rate (/s) counter for bmrtotv6txpktsudp
bmrtotv4rxpktsudp	<Double>	Read-only	Total number of MAP-T BMR V4 UDP Recieved packets.
bmrv4rxpktsudprate	<Double>	Read-only	Rate (/s) counter for bmrtotv4rxpktsudp
bmrtotv4txpktsudp	<Double>	Read-only	Total number of MAP-T BMR V4

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			UDP Transmitted packets.
bmrv4txpktsudprate	<Double>	Read-only	Rate (/s) counter for bmrtotv4txpktsudp
bmrtotv6rxpktsicmp	<Double>	Read-only	Total number of MAP-T BMR V6 ICMP Recieved packets.
bmrv6rxpktsicmprate	<Double>	Read-only	Rate (/s) counter for bmrtotv6rxpktsicmp
bmrtotv6txpktsicmp	<Double>	Read-only	Total number of MAP-T BMR V6 ICMP Transmitted packets.
bmrv6txpktsicmprate	<Double>	Read-only	Rate (/s) counter for bmrtotv6txpktsicmp
bmrtotv4rxpktsicmp	<Double>	Read-only	Total number of MAP-T BMR V4 ICMP Recieved packets.
bmrv4rxpktsicmprate	<Double>	Read-only	Rate (/s) counter for bmrtotv4rxpktsicmp
bmrtotv4txpktsicmp	<Double>	Read-only	Total number of MAP-T BMR V4 ICMP Transmitted packets.
bmrv4txpktsicmprate	<Double>	Read-only	Rate (/s) counter for bmrtotv4txpktsicmp

Operations

(click to see Properties)

- GET (ALL)
- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/mapbmr **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/mapbmr? **args=name: <String_value> ,detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get mapbmr resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/mapbmr? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "mapbmr": [ {

"name":<String_value>,

"bmrtotv4txpkts":<Double_value>,

"bmrtotv4rxpktsicmp":<Double_value>,

"bmrtotv6rxpktsicmp":<Double_value>,

"bmrtotv6txpkts":<Double_value>,

"bmrtotv4rxpkts":<Double_value>,

"bmrtotv4txpktsicmp":<Double_value>,

"bmrv6rxpktsudprate":<Double_value>,

"bmrv4txpktsrate":<Double_value>,

"bmrtotv6txpktsicmp":<Double_value>,

"bmrv4rxpktstcprate":<Double_value>,

"bmrv4rxpktsicmprate":<Double_value>,
```

```
"bmrtotv6rxpkts":<Double_value>,

"bmrv6rxpktstcprate":<Double_value>,

"bmrv6rxpktsicmprate":<Double_value>,

"bmrv4rxpktsudprate":<Double_value>,

"bmrv6txpktsrate":<Double_value>,

"bmrtotv4txpktstcp":<Double_value>,

"bmrtotv6txpktstcp":<Double_value>,

"bmrv6txpktstcprate":<Double_value>,

"bmrtotv4rxpktstcp":<Double_value>,

"bmrv6txpktsicmprate":<Double_value>,

"bmrv4txpktsudprate":<Double_value>,

"bmrv6rxpktsrate":<Double_value>,

"bmrtotv6rxpktstcp":<Double_value>,

"bmrtotv6txpktsudp":<Double_value>,

"bmrv6txpktsudprate":<Double_value>,

"bmrv4rxpktsrate":<Double_value>,

"bmrv4txpktstcprate":<Double_value>,

"bmrv4txpktsicmprate":<Double_value>,

"bmrtotv4txpktsudp":<Double_value>,

"bmrtotv6rxpktsudp":<Double_value>,

"bmrtotv4rxpktsudp":<Double_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/stat/mapbmr/ name_value><String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "mapbmr": [ {

"name":<String_value>,

"bmrtotv4txpkts":<Double_value>,

"bmrtotv4rxpktsicmp":<Double_value>,

"bmrtotv6rxpktsicmp":<Double_value>,

"bmrtotv6txpkts":<Double_value>,

"bmrtotv4rxpkts":<Double_value>,

"bmrtotv4txpktsicmp":<Double_value>,

"bmrv6rxpktsudprate":<Double_value>,

"bmrv4txpktsrate":<Double_value>,

"bmrtotv6txpktsicmp":<Double_value>,
```

```
"bmrv4rxpktstcprate":<Double_value>,

"bmrv4rxpktsicmprate":<Double_value>,

"bmrtotv6rxpkts":<Double_value>,

"bmrv6rxpktstcprate":<Double_value>,

"bmrv6rxpktsicmprate":<Double_value>,

"bmrv4rxpktsudprate":<Double_value>,

"bmrv6txpktsrate":<Double_value>,

"bmrtotv4txpktstcp":<Double_value>,

"bmrtotv6txpktstcp":<Double_value>,

"bmrv6txpktstcprate":<Double_value>,

"bmrtotv4rxpktstcp":<Double_value>,

"bmrv6txpktsicmprate":<Double_value>,

"bmrv4txpktsudprate":<Double_value>,

"bmrv6rxpktsrate":<Double_value>,

"bmrtotv6rxpktstcp":<Double_value>,

"bmrtotv6txpktsudp":<Double_value>,

"bmrv6txpktsudprate":<Double_value>,

"bmrv4rxpktsrate":<Double_value>,

"bmrv4txpktstcprate":<Double_value>,

"bmrv4txpktsicmprate":<Double_value>,

"bmrtotv4txpktsudp":<Double_value>,

"bmrtotv6rxpktsudp":<Double_value>,
```

```
"bmrtotv4rxpktsudp":<Double_value>

}]}
```

mapdomain

Statistics for MAP-T Map Domain resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	An integer specifying the VLAN identification number (VID). Possible values: 1 through 4094. Minimum length = 1 Maximum length = 127
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full
maptotv6rxpktstcp	<Double>	Read-only	Total number of MAP-T IPv6 TCP Recieved packets.
mapv6rxpktstcprate	<Double>	Read-only	Rate (/s) counter for maptotv6rxpktstcp
maptotv6txpktstcp	<Double>	Read-only	Total number of MAP-T IPv6 TCP Transmitted packets.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
mapv6txpktstcprate	<Double>	Read-only	Rate (/s) counter for maptotv6txpktstcp
maptotv6rxbytestcp	<Double>	Read-only	Total number of MAP-T IPv6 TCP Recieved Bytes.
mapv6rxbytestcprate	<Double>	Read-only	Rate (/s) counter for maptotv6rxbytestcp
maptotv6txbytestcp	<Double>	Read-only	Total number of MAP-T IPv6 TCP Transmitted Bytes.
mapv6txbytestcprate	<Double>	Read-only	Rate (/s) counter for maptotv6txbytestcp
maptotv4rxpktstcp	<Double>	Read-only	Total number of MAP-T IPv4 TCP Recieved packets.
mapv4rxpktstcprate	<Double>	Read-only	Rate (/s) counter for maptotv4rxpktstcp
maptotv4txpktstcp	<Double>	Read-only	Total number of MAP-T IPv4 TCP Transmitted packets.
mapv4txpktstcprate	<Double>	Read-only	Rate (/s) counter for maptotv4txpktstcp
maptotv4rxbytestcp	<Double>	Read-only	Total number of MAP-T IPv4 TCP Recieved Bytes.
mapv4rxbytestcprate	<Double>	Read-only	Rate (/s) counter for maptotv4rxbytestcp
maptotv4txbytestcp	<Double>	Read-only	Total number of MAP-T IPv4 TCP Transmitted Bytes.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
mapv4txbytestcprate	<Double>	Read-only	Rate (/s) counter for maptotv4txbytestcp
maptotv6rxpktsudp	<Double>	Read-only	Total number of MAP-T IPv6 UDP Recieved packets.
mapv6rxpktsudprate	<Double>	Read-only	Rate (/s) counter for maptotv6rxpktsudp
maptotv6txpktsudp	<Double>	Read-only	Total number of MAP-T IPv6 UDP Transmitted packets.
mapv6txpktsudprate	<Double>	Read-only	Rate (/s) counter for maptotv6txpktsudp
maptotv6rxbytesudp	<Double>	Read-only	Total number of MAP-T IPv6 UDP Recieved Bytes.
mapv6rxbytesudprate	<Double>	Read-only	Rate (/s) counter for maptotv6rxbytesudp
maptotv6txbytesudp	<Double>	Read-only	Total number of MAP-T IPv6 UDP Transmitted Bytes.
mapv6txbytesudprate	<Double>	Read-only	Rate (/s) counter for maptotv6txbytesudp
maptotv4rxpktsudp	<Double>	Read-only	Total number of MAP-T IPv4 UDP Recieved packets.
mapv4rxpktsudprate	<Double>	Read-only	Rate (/s) counter for maptotv4rxpktsudp
maptotv4txpktsudp	<Double>	Read-only	Total number of MAP-T IPv4 UDP Transmitted packets.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
mapv4txpktsudprate	<Double>	Read-only	Rate (/s) counter for maptotv4txpktsudp
maptotv4rxbytesudp	<Double>	Read-only	Total number of MAP-T IPv4 UDP Recieved Bytes.
mapv4rxbytesudprate	<Double>	Read-only	Rate (/s) counter for maptotv4rxbytesudp
maptotv4txbytesudp	<Double>	Read-only	Total number of MAP-T IPv4 UDP Transmitted Bytes.
mapv4txbytesudprate	<Double>	Read-only	Rate (/s) counter for maptotv4txbytesudp
maptotv6rxpktsicmp	<Double>	Read-only	Total number of MAP-T IPv6 ICMP Recieved packets.
mapv6rxpktsicmprate	<Double>	Read-only	Rate (/s) counter for maptotv6rxpktsicmp
maptotv6txpktsicmp	<Double>	Read-only	Total number of MAP-T IPv6 ICMP Transmitted packets.
mapv6txpktsicmprate	<Double>	Read-only	Rate (/s) counter for maptotv6txpktsicmp
maptotv6rxbytesicmp	<Double>	Read-only	Total number of MAP-T IPv6 ICMP Recieved Bytes.
mapv6rxbytesicmprate	<Double>	Read-only	Rate (/s) counter for maptotv6rxbytesicmp
maptotv6txbytesicmp	<Double>	Read-only	Total number of MAP-T IPv6 ICMP Transmitted Bytes.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
mapv6txbytesicmprate	<Double>	Read-only	Rate (/s) counter for maptotv6txbytesicmp
maptotv4rxpktsicmp	<Double>	Read-only	Total number of MAP-T IPv4 ICMP Recieved packets.
mapv4rxpktsicmprate	<Double>	Read-only	Rate (/s) counter for maptotv4rxpktsicmp
maptotv4txpktsicmp	<Double>	Read-only	Total number of MAP-T IPv4 ICMP Transmitted packets.
mapv4txpktsicmprate	<Double>	Read-only	Rate (/s) counter for maptotv4txpktsicmp
maptotv4rxbytesicmp	<Double>	Read-only	Total number of MAP-T IPv4 ICMP Recieved Bytes.
mapv4rxbytesicmprate	<Double>	Read-only	Rate (/s) counter for maptotv4rxbytesicmp
maptotv4txbytesicmp	<Double>	Read-only	Total number of MAP-T IPv4 ICMP Transmitted Bytes.
mapv4txbytesicmprate	<Double>	Read-only	Rate (/s) counter for maptotv4txbytesicmp
maptotv6rxpkts	<Double>	Read-only	Total number of MAP-T V6 Recieved packets.
mapv6rxpktsrate	<Double>	Read-only	Rate (/s) counter for maptotv6rxpkts
maptotv6txpkts	<Double>	Read-only	Total number of MAP-T V6 Transmitted packets.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
mapv6txpktsrate	<Double>	Read-only	Rate (/s) counter for maptotv6txpkts
maptotv4rxpkts	<Double>	Read-only	Total number of MAP-T V4 Recieved packets.
mapv4rxpktsrate	<Double>	Read-only	Rate (/s) counter for maptotv4rxpkts
maptotv4txpkts	<Double>	Read-only	Total number of MAP-T V4 Transmitted packets.
mapv4txpktsrate	<Double>	Read-only	Rate (/s) counter for maptotv4txpkts

Operations

(click to see Properties)

- GET (ALL)
- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/mapdomain **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/mapdomain? **args=name: <String_value> ,detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get mapdomain resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/mapdomain? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "mapdomain": [ {

"name":<String_value>,
```

```
"mapv6txbytesudprate":<Double_value>,

"mapv6txpktstcprate":<Double_value>,

"maptotv4rxpktstcp":<Double_value>,

"mapv6txpktsicmprate":<Double_value>,

"mapv4txpktsudprate":<Double_value>,

"maptotv6txbytesicmp":<Double_value>,

"mapv6rxpktsrate":<Double_value>,

"maptotv4txbytesicmp":<Double_value>,

"maptotv6rxpktstcp":<Double_value>,

"mapv4rxbytesicmprate":<Double_value>,

"maptotv4txpktstcp":<Double_value>,

"maptotv6rxbytesicmp":<Double_value>,

"maptotv4rxbytesicmp":<Double_value>,

"maptotv6txpktstcp":<Double_value>,

"mapv4txbytestcprate":<Double_value>,

"mapv6txbytestcprate":<Double_value>,

"maptotv6rxpktsudp":<Double_value>,

"maptotv4rxpktsudp":<Double_value>,

"mapv6rxbytesicmprate":<Double_value>,

"maptotv6txpktsudp":<Double_value>,

"mapv6txpktsudprate":<Double_value>,

"mapv4rxpktsrate":<Double_value>,
```

```
"mapv4txpktstcprate":<Double_value>,

"mapv4txpktsicmprate":<Double_value>,

"mapv4txbytesudprate":<Double_value>,

"maptotv4txpktsudp":<Double_value>,

"maptotv4rxpkts":<Double_value>,

"maptotv6txbytestcp":<Double_value>,

"maptotv4txpktsicmp":<Double_value>,

"maptotv6txpktsicmp":<Double_value>,

"mapv6rxpktsudprate":<Double_value>,

"mapv4txpktsrate":<Double_value>,

"mapv4rxbytesudprate":<Double_value>,

"maptotv4txbytestcp":<Double_value>,

"mapv4rxpktstcprate":<Double_value>,

"maptotv6rxpkts":<Double_value>,

"mapv4rxpktsicmprate":<Double_value>,

"maptotv6rxbytestcp":<Double_value>,

"maptotv4txpkts":<Double_value>,

"mapv6rxbytestcprate":<Double_value>,

"maptotv4rxpktsicmp":<Double_value>,

"maptotv6rxpktsicmp":<Double_value>,

"mapv6txbytesicmprate":<Double_value>,

"maptotv6txpkts":<Double_value>,
```

```
"maptotv4rxbytestcp":<Double_value>,

"maptotv4txbytesudp":<Double_value>,

"mapv4txbytesicmprate":<Double_value>,

"mapv4rxbytestcprate":<Double_value>,

"maptotv6txbytesudp":<Double_value>,

"mapv6rxpktstcprate":<Double_value>,

"maptotv4rxbytesudp":<Double_value>,

"mapv6rxpktsicmprate":<Double_value>,

"mapv6rxbytesudprate":<Double_value>,

"mapv4rxpktsudprate":<Double_value>,

"mapv6txpktsrate":<Double_value>,

"maptotv6rxbytesudp":<Double_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/stat/mapdomain/ name_value><String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "mapdomain": [ {

"name":<String_value>,

"mapv6txbytesudprate":<Double_value>,

"mapv6txpktstcprate":<Double_value>,

"maptotv4rxpktstcp":<Double_value>,

"mapv6txpktsicmprate":<Double_value>,

"mapv4txpktsudprate":<Double_value>,

"maptotv6txbytesicmp":<Double_value>,

"mapv6rxpktsrate":<Double_value>,

"maptotv4txbytesicmp":<Double_value>,

"maptotv6rxpktstcp":<Double_value>,

"mapv4rxbytesicmprate":<Double_value>,

"maptotv4txpktstcp":<Double_value>,

"maptotv6rxbytesicmp":<Double_value>,

"maptotv4rxbytesicmp":<Double_value>,

"maptotv6txpktstcp":<Double_value>,

"mapv4txbytestcprate":<Double_value>,

"mapv6txbytestcprate":<Double_value>,

"maptotv6rxpktsudp":<Double_value>,

"maptotv4rxpktsudp":<Double_value>,
```

```
"mapv6rxbytesicmprate":<Double_value>,

"maptotv6txpktsudp":<Double_value>,

"mapv6txpktsudprate":<Double_value>,

"mapv4rxpktsrate":<Double_value>,

"mapv4txpktstcprate":<Double_value>,

"mapv4txpktsicmprate":<Double_value>,

"mapv4txbytesudprate":<Double_value>,

"maptotv4txpktsudp":<Double_value>,

"maptotv4rxpkts":<Double_value>,

"maptotv6txbytestcp":<Double_value>,

"maptotv4txpktsicmp":<Double_value>,

"maptotv6txpktsicmp":<Double_value>,

"mapv6rxpktsudprate":<Double_value>,

"mapv4txpktsrate":<Double_value>,

"mapv4rxbytesudprate":<Double_value>,

"maptotv4txbytestcp":<Double_value>,

"mapv4rxpktstcprate":<Double_value>,

"maptotv6rxpkts":<Double_value>,

"mapv4rxpktsicmprate":<Double_value>,

"maptotv6rxbytestcp":<Double_value>,

"maptotv4txpkts":<Double_value>,

"mapv6rxbytestcprate":<Double_value>,
```

```
"maptotv4rxpktsicmp":<Double_value>,

"maptotv6rxpktsicmp":<Double_value>,

"mapv6txbytesicmprate":<Double_value>,

"maptotv6txpkts":<Double_value>,

"maptotv4rxbytestcp":<Double_value>,

"maptotv4txbytesudp":<Double_value>,

"mapv4txbytesicmprate":<Double_value>,

"mapv4rxbytestcprate":<Double_value>,

"maptotv6txbytesudp":<Double_value>,

"mapv6rxpktstcprate":<Double_value>,

"maptotv4rxbytesudp":<Double_value>,

"mapv6rxpktsicmprate":<Double_value>,

"mapv6rxbytesudprate":<Double_value>,

"mapv4rxpktsudprate":<Double_value>,

"mapv6txpktsrate":<Double_value>,

"maptotv6rxbytesudp":<Double_value>

}]}
```

nat64

Statistics for nat64 config resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full
nat64tottcpsessions	<Double>	Read-only	Total number of TCP sessions created by NAT64.
nat64tcpsessionsrate	<Double>	Read-only	Rate (/s) counter for nat64tottcpsessions
nat64totudpsessions	<Double>	Read-only	Total number of UDP sessions created by NAT64.
nat64udpsessionsrate	<Double>	Read-only	Rate (/s) counter for nat64totudpsessions
nat64toticmpsessions	<Double>	Read-only	Total number of ICMP sessions created by NAT64.
nat64icmpsessionsrate	<Double>	Read-only	Rate (/s) counter for nat64toticmpsessions
nat64totsessions	<Double>	Read-only	Total number of sessions created by NAT64.
nat64sessionsrate	<Double>	Read-only	Rate (/s) counter for nat64totsessions

Operations

(click to see Properties)

- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/nat64 **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/nat64? **args=detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get nat64 resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/nat64? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "nat64": [ {

"nat64sessionsrate":<Double_value>,

"nat64tottcpsessions":<Double_value>,

"nat64icmpsessionsrate":<Double_value>,

"nat64udpsessionsrate":<Double_value>,

"nat64toticmpsessions":<Double_value>,

"nat64totsessions":<Double_value>,

"nat64tcpsessionsrate":<Double_value>,

"nat64totudpsessions":<Double_value>

}]}
```

rnat

Statistics for RNAT configured route resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full
rnattotrxbytes	<Double>	Read-only	Bytes received during RNAT sessions.
rnatrxbytesrate	<Double>	Read-only	Rate (/s) counter for rnattotrxbytes
rnattottxbytes	<Double>	Read-only	Bytes sent during RNAT sessions.
rnattxbytesrate	<Double>	Read-only	Rate (/s) counter for rnattottxbytes
rnattotrxpkts	<Double>	Read-only	Packets received during RNAT sessions.
rnatrxpktsrate	<Double>	Read-only	Rate (/s) counter for rnattotrxpkts
rnattottxpkts	<Double>	Read-only	Packets sent during RNAT sessions.
rnattxpktsrate	<Double>	Read-only	Rate (/s) counter for rnattottxpkts
rnattottxsyn	<Double>	Read-only	Requests for connections sent during RNAT sessions.
rnattxsynrate	<Double>	Read-only	Rate (/s) counter for rnattottxsyn
rnatcursessions	<Double>	Read-only	Currently active RNAT sessions.

Operations

(click to see Properties)

- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/rnat **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/rnat? **args=detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get rnat resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/rnat? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "rnat": [ {

"rnatcursessions":<Double_value>,

"rnattottxbytes":<Double_value>,

"rnattxsynrate":<Double_value>,

"rnatrxpktsrate":<Double_value>,

"rnattxpktsrate":<Double_value>,

"rnattotrxbytes":<Double_value>,

"rnattottxsyn":<Double_value>,

"rnatrxbytesrate":<Double_value>,

"rnattotrxpkts":<Double_value>,

"rnattxbytesrate":<Double_value>,

"rnattottxpkts":<Double_value>
```

```
}]}
```

rnat6

Statistics for IPv6 RNAT configured route resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full
rnat6totrxbytes	<Double>	Read-only	Bytes received during RNAT6 sessions.
rnat6rxbytesrate	<Double>	Read-only	Rate (/s) counter for rnat6totrxbytes
rnat6tottxbytes	<Double>	Read-only	Bytes sent during RNAT6 sessions.
rnat6txbytesrate	<Double>	Read-only	Rate (/s) counter for rnat6tottxbytes
rnat6totrxpkts	<Double>	Read-only	Packets received during RNAT6 sessions.
rnat6rxpktsrate	<Double>	Read-only	Rate (/s) counter for rnat6totrxpkts
rnat6tottxpkts	<Double>	Read-only	Packets sent during RNAT6 sessions.
rnat6txpktsrate	<Double>	Read-only	Rate (/s) counter for rnat6tottxpkts

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
rnat6tottxsyn	<Double>	Read-only	Requests for connections sent during RNAT6 sessions.
rnat6txsynrate	<Double>	Read-only	Rate (/s) counter for rnat6tottxsyn
rnat6cursessions	<Double>	Read-only	Currently active RNAT6 sessions.

Operations

(click to see Properties)

- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/rnat6 **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/rnat6? **args=detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get rnat6 resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/rnat6? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "rnat6": [ {

"rnat6totrxpkts":<Double_value>,

"rnat6tottxpkts":<Double_value>,

"rnat6txpktsrate":<Double_value>,

"rnat6cursessions":<Double_value>,

"rnat6txbytesrate":<Double_value>,
```

```
"rnat6tottxsyn":<Double_value>,

"rnat6rxbytesrate":<Double_value>,

"rnat6tottxbytes":<Double_value>,

"rnat6rxpktsrate":<Double_value>,

"rnat6totrxbytes":<Double_value>,

"rnat6txsynrate":<Double_value>

}]}
```

rnatip

Statistics for RNAT ipaddress resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
Rnatip	<String>	Read-write	Specifies the NAT IP address of the configured RNAT entry for which you want to see the statistics. If you do not specify an IP address, this displays the statistics for all the configured RNAT entries. Minimum length = 1
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
iptd	<Double>	Read-only	Traffic domain for ipaddr.
iprnattotrxbytes	<Double>	Read-only	Bytes received on this IP address during RNAT sessions.
iprnatrxbytesrate	<Double>	Read-only	Rate (/s) counter for iprnattotrxbytes
iprnattottxbytes	<Double>	Read-only	Bytes sent from this IP address during RNAT sessions.
iprnattxbytesrate	<Double>	Read-only	Rate (/s) counter for iprnattottxbytes
iprnattotrxpkts	<Double>	Read-only	Packets received on this IP address during RNAT sessions.
iprnatrxpktsrate	<Double>	Read-only	Rate (/s) counter for iprnattotrxpkts
iprnattottxpkts	<Double>	Read-only	Packets sent from this IP address during RNAT sessions.
iprnattxpktsrate	<Double>	Read-only	Rate (/s) counter for iprnattottxpkts
iprnattottxsyn	<Double>	Read-only	Requests for connections sent from this IP address during RNAT sessions.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
iprnattxsynrate	<Double>	Read-only	Rate (/s) counter for iprnattottxsyn
iprnatcursessions	<Double>	Read-only	Currently active RNAT sessions started from this IP address.

Operations

(click to see Properties)

- GET (ALL)
- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/rnatip **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/rnatip? **args=Rnatip: <String_value> ,detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get rnatip resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/rnatip? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "rnatip": [ {

"Rnatip":<String_value>,

"iprnatrxpktsrate":<Double_value>,

"iprnatrxbytesrate":<Double_value>,

"iprnattottxpkts":<Double_value>,

"iprnattotrxpkts":<Double_value>,
```

```
"iprnattottxbytes":<Double_value>,

"iprnattotrxbytes":<Double_value>,

"iptd":<Double_value>,

"iprnattottxsyn":<Double_value>,

"iprnatcursessions":<Double_value>,

"iprnattxsynrate":<Double_value>,

"iprnattxbytesrate":<Double_value>,

"iprnattxpktsrate":<Double_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/stat/rnatip/ Rnatip_value><String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "rnatip": [ {

"Rnatip":<String_value>,

"iprnatrxpktsrate":<Double_value>,

"iprnatrxbytesrate":<Double_value>,

"iprnattottxpkts":<Double_value>,

"iprnattotrxpkts":<Double_value>,

"iprnattottxbytes":<Double_value>,

"iprnattotrxbytes":<Double_value>,

"iptd":<Double_value>,

"iprnattottxsyn":<Double_value>,

"iprnatcursessions":<Double_value>,

"iprnattxsynrate":<Double_value>,

"iprnattxbytesrate":<Double_value>,

"iprnattxpktsrate":<Double_value>

}]}
```

tunnelip

Statistics for TUNNEL Remote ipaddress resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
tunnelip	<String>	Read-write	remote IP address of the configured tunnel. Minimum length = 1
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full
tnltotrxpkts	<Double>	Read-only	Total number of packets received on the tunnel.
tnlrxpktsrate	<Double>	Read-only	Rate (/s) counter for tnltotrxpkts
tnltottxpkts	<Double>	Read-only	Total number of packets transmitted on the tunnel.
tnltxpktsrate	<Double>	Read-only	Rate (/s) counter for tnltottxpkts
tnltotrxbytes	<Double>	Read-only	Total number of bytes received on the tunnel.
tnlrxbytesrate	<Double>	Read-only	Rate (/s) counter for tnltotrxbytes
tnltottxbytes	<Double>	Read-only	Total number of bytes transmitted on the tunnel.
tnltxbytesrate	<Double>	Read-only	Rate (/s) counter for tnltottxbytes

Operations

(click to see Properties)

- GET (ALL)
- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/tunnelip **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/tunnelip? **args=tunnelip: <String_value> ,detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get tunnelip resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/tunnelip? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "tunnelip": [ {

"tunnelip":<String_value>,

"tnltottxbytes":<Double_value>,

"tnlrxbytesrate":<Double_value>,

"tnltxbytesrate":<Double_value>,

"tnltotrxpkts":<Double_value>,

"tnlrxpktsrate":<Double_value>,

"tnltxpktsrate":<Double_value>,

"tnltottxpkts":<Double_value>,

"tnltotrxbytes":<Double_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/stat/tunnelip/ tunnelip_value><String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "tunnelip": [ {

"tunnelip":<String_value>,

"tnltottxbytes":<Double_value>,

"tnlrxbytesrate":<Double_value>,

"tnltxbytesrate":<Double_value>,

"tnltotrxpkts":<Double_value>,

"tnlrxpktsrate":<Double_value>,

"tnltxpktsrate":<Double_value>,

"tnltottxpkts":<Double_value>,

"tnltotrxbytes":<Double_value>

}]}
```

tunnelip6

Statistics for TUNNEL Remote ip6address resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
tunnelip6	<String>	Read-write	remote IPv6 address of the configured tunnel. Minimum length = 1
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full
tnltotrxpkts	<Double>	Read-only	Total number of packets received on the tunnel.
tnlrxpktsrate	<Double>	Read-only	Rate (/s) counter for tnltotrxpkts
tnltottxpkts	<Double>	Read-only	Total number of packets transmitted on the tunnel.
tnltxpktsrate	<Double>	Read-only	Rate (/s) counter for tnltottxpkts
tnltotrxbytes	<Double>	Read-only	Total number of bytes received on the tunnel.
tnlrxbytesrate	<Double>	Read-only	Rate (/s) counter for tnltotrxbytes
tnltottxbytes	<Double>	Read-only	Total number of bytes transmitted on the tunnel.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
tnltxbytesrate	<Double>	Read-only	Rate (/s) counter for tnltottxbytes

Operations

(click to see Properties)

- GET (ALL)
- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/tunnelip6 **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/tunnelip6? **args=tunnelip6: <String_value> ,detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get tunnelip6 resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/tunnelip6? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "tunnelip6": [ {

"tunnelip6":<String_value>,

"tnlrxpktsrate":<Double_value>,

"tnltxpktsrate":<Double_value>,

"tnltottxpkts":<Double_value>,

"tnltotrxbytes":<Double_value>,
```

```
"tnltottxbytes":<Double_value>,

"tnlrxbytesrate":<Double_value>,

"tnltotrxpkts":<Double_value>,

"tnltxbytesrate":<Double_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/stat/tunnelip6/ tunnelip6_value><String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "tunnelip6": [ {

"tunnelip6":<String_value>,

"tnlrxpktsrate":<Double_value>,

"tnltxpktsrate":<Double_value>,

"tnltottxpkts":<Double_value>,

"tnltotrxbytes":<Double_value>,
```

```
"tnltottxbytes":<Double_value>,

"tnlrxbytesrate":<Double_value>,

"tnltotrxpkts":<Double_value>,

"tnltxbytesrate":<Double_value>

}]}
```

vlan

Statistics for "VLAN" resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
id	<Integer>	Read-write	An integer specifying the VLAN identification number (VID). Possible values: 1 through 4094. Minimum value = 1 Maximum value = 4094
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full
vlantotrxpkts	<Double>	Read-only	Packets received on the VLAN.
vlanrxpktsrate	<Double>	Read-only	Rate (/s) counter for vlantotrxpkts

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
vlantotrxbytes	<Double>	Read-only	Bytes of data received on the VLAN.
vlanrxbytesrate	<Double>	Read-only	Rate (/s) counter for vlantotrxbytes
vlantottxpkts	<Double>	Read-only	Packets transmitted on the VLAN.
vlantxpktsrate	<Double>	Read-only	Rate (/s) counter for vlantottxpkts
vlantottxbytes	<Double>	Read-only	Bytes of data transmitted on the VLAN.
vlantxbytesrate	<Double>	Read-only	Rate (/s) counter for vlantottxbytes
vlantotdroppedpkts	<Double>	Read-only	Inbound packets dropped by the VLAN upon reception.
vlantotbroadcastpkts	<Double>	Read-only	Broadcast packets sent and received on the VLAN.

Operations

(click to see Properties)

- GET (ALL)
- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/vlan **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/vlan? **args=id: <Integer_value> ,detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get vlan resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/vlan? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vlan": [ {

"id":<Integer_value>,

"vlantotrxpkts":<Double_value>,

"vlanrxbytesrate":<Double_value>,

"vlantxpktsrate":<Double_value>,

"vlantotbroadcastpkts":<Double_value>,

"vlantotdroppedpkts":<Double_value>,

"vlantottxbytes":<Double_value>,

"vlantxbytesrate":<Double_value>,

"vlantottxpkts":<Double_value>,

"vlanrxpktsrate":<Double_value>,

"vlantotrxbytes":<Double_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/stat/vlan/ id_value><Integer> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vlan": [ {

"id":<Integer_value>,

"vlantotrxpkts":<Double_value>,

"vlanrxbytesrate":<Double_value>,

"vlantxpktsrate":<Double_value>,

"vlantotbroadcastpkts":<Double_value>,

"vlantotdroppedpkts":<Double_value>,

"vlantottxbytes":<Double_value>,

"vlantxbytesrate":<Double_value>,

"vlantottxpkts":<Double_value>,

"vlanrxpktsrate":<Double_value>,

"vlantotrxbytes":<Double_value>

}]}
```

vxlan

Statistics for "VXLAN" resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
id	<Integer>	Read-write	An integer specifying the VXLAN identification number (VNID). Minimum value = 1 Maximum value = 16777215
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full
vxlantotrxpkts	<Double>	Read-only	Packets received on the VXLAN.
vxlanrxpktsrate	<Double>	Read-only	Rate (/s) counter for vxlantotrxpkts
vxlantotrxbytes	<Double>	Read-only	Bytes of data received on the VXLAN.
vxlanrxbytesrate	<Double>	Read-only	Rate (/s) counter for vxlantotrxbytes
vxlantottxpkts	<Double>	Read-only	Packets transmitted on the VXLAN.
vxlantxpktsrate	<Double>	Read-only	Rate (/s) counter for vxlantottxpkts
vxlantottxbytes	<Double>	Read-only	Bytes of data transmitted on the VXLAN.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
vxlantxbytesrate	<Double>	Read-only	Rate (/s) counter for vxlantottxbytes

Operations

(click to see Properties)

- GET (ALL)
- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/vxlan **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/vxlan? **args=id: <Integer_value> ,detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get vxlan resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/vxlan? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vxlan": [ {

"id":<Integer_value>,

"vxlantottxbytes":<Double_value>,

"vxlantottxpkts":<Double_value>,

"vxlanrxbytesrate":<Double_value>,

"vxlanrxpktsrate":<Double_value>,

"vxlantotrxbytes":<Double_value>,
```

```
"vxlantotrxpkts":<Double_value>,

"vxlantxpktsrate":<Double_value>,

"vxlantxbytesrate":<Double_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/stat/vxlan/ id_value><Integer> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vxlan": [ {

"id":<Integer_value>,

"vxlantottxbytes":<Double_value>,

"vxlantottxpkts":<Double_value>,

"vxlanrxbytesrate":<Double_value>,

"vxlanrxpktsrate":<Double_value>,

"vxlantotrxbytes":<Double_value>,
```

```
"vxlantotrxpkts":<Double_value>,

"vxlantxpktsrate":<Double_value>,

"vxlantxbytesrate":<Double_value>

}]}
```

ns

NS

System/Global level statistics.

NAME	DESCRIPTION
ns	Statistics for ns.
nsacl	Statistics for ACL entry resource.
nsacl6	Statistics for ACL6 entry resource.
nslimitidentifier	Statistics for limit Identifier resource.
nsmemory	
nspartition	Statistics for admin partition resource.
nspbr	Statistics for Policy Based Routing(PBR) entry resource.
nspbr6	Statistics for PBR6 entry resource.
nssimpleacl	Statistics for simple ACL resource.
nssimpleacl6	Statistics for simple ACL6 resource.
nstrafficdomain	Statistics for Traffic Domain resource.

ns

Statistics for ns.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full
rescpuusagepcnt	<Double>	Read-only	Average CPU utilization percentage. Not applicable for a single-CPU system.
cpuusagepcnt	<Double>	Read-only	CPU utilization percentage.
cachemaxmemorykb	<Double>	Read-only	Largest amount of memory the Citrix ADC can dedicate to caching, up to 50% of available memory. A 0 value disables caching, but the caching module continues to run.
delcmpratio	<Double>	Read-only	Ratio of compressible data received to compressed data transmitted.If this ratio is one (uncmp:1.0) that means compression is disabled or we are not able to compress

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			even a single compressible packet.
rescpuusage	<Double>	Read-only	Shows average CPU utilization percentage if more than 1 CPU is present.
cpuusage	<Double>	Read-only	CPU utilization percentage.
resmemusage	<Double>	Read-only	Percentage of memory utilization on Citrix ADC.
comptotaldatacompressionratio	<Double>	Read-only	Ratio of total HTTP data received to total HTTP data transmitted.
compratio	<Double>	Read-only	Ratio of the compressible data received from the server to the compressed data sent to the client.
cacheutilizedmemorykb	<Double>	Read-only	Amount of memory the integrated cache is currently using.
cachemaxmemoryactivekb	<Double>	Read-only	Currently active value of maximum memory
cache64maxmemorykb	<Double>	Read-only	Largest amount of memory the Citrix ADC can dedicate to caching, up to 50% of available memory. A 0 value disables caching, but the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			caching module continues to run.
cachepercentoriginbandwidthsaved	<Double>	Read-only	Percentage of origin bandwidth saved, expressed as number of bytes served from the integrated cache divided by all bytes served. The assumption is that all compression is done in the Citrix ADC.
cachetotmisses	<Double>	Read-only	Intercepted HTTP requests requiring fetches from origin server.
cachemissesrate	<Double>	Read-only	Rate (/s) counter for cachetotmisses
cachetothits	<Double>	Read-only	Responses served from the integrated cache. These responses match a policy with a CACHE action.
cachehitsrate	<Double>	Read-only	Rate (/s) counter for cachetothits
memusagepcnt	<Double>	Read-only	Percentage of memory utilization on Citrix ADC.
memuseinmb	<Double>	Read-only	Main memory currently in use, in megabytes.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
mgmtcpuusagepcnt	<Double>	Read-only	Average Management CPU utilization percentage.
pktcpuusagepcnt	<Double>	Read-only	Average CPU utilization percentage for all packet engines excluding management PE.
starttimelocal	<String>	Read-only	Time (in local timezone format) when the Citrix ADC was last started.
starttime	<String>	Read-only	Time when the Citrix ADC was last started.
transtime	<String>	Read-only	Time when the last master state transition occurred. You can use this statistic for debugging.
hacurstate	<String>	Read-only	State of the HA node, based on its health, in a high availability setup. Possible values are: UP - Indicates that the node is accessible and can function as either a primary or secondary node. DISABLED - Indicates that the high availability status of the node

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			has been manually disabled. Synchronization and propagation cannot take place between the peer nodes. INIT - Indicates that the node is in the process of becoming part of the high availability configuration. PARTIALFAIL - Indicates that one of the high availability monitored interfaces has failed because of a card or link failure. This state triggers a failover. COMPLETEFAIL - Indicates that all the interfaces of the node are unusable, because the interfaces on which high availability monitoring is enabled are not connected or are manually disabled. This state triggers a failover. DUMB - Indicates that the node is in listening mode. It does not participate in high availability transitions or transfer configuration from the peer node. This

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			is a configured value, not a statistic. PARTIALFAILSSL - Indicates that the SSL card has failed. This state triggers a failover. ROUTEMONITORFAIL - Indicates that the route monitor has failed. This state triggers a failover.
hacurmasterstate	<String>	Read-only	Indicates the high availability state of the node. Possible values are: STAYSECONDARY - Indicates that the selected node remains the secondary node in a high availability setup. In this case a forced failover does not change the state but, instead, returns an appropriate error message. This is a configured value and not a statistic. PRIMARY - Indicates that the selected node is the primary node in a high availability setup. SECONDARY - Indicates that the selected node is the secondary node in a high availability

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			setup. CLAIMING - Indicates that the secondary node is in the process of taking over as the primary node. This is the intermediate state in the transition of the secondary node to primary status. FORCE CHANGE - Indicates that the secondary node is forcibly changing its status to primary due to a forced failover issued on the secondary node.
sslnumcardsup	<Double>	Read-only	Number of SSL cards that are UP. If the number of cards UP is lower than a threshold, a failover is initiated.
sslcards	<Double>	Read-only	Number of SSL crypto cards present on the Citrix ADC.
disk0perusage	<Double>	Read-only	Used space in /flash partition of the disk, as a percentage. This is a critical counter. You can configure /flash Used (%) by using the Set snmp alarm DISK-USAGE-HIGH command.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
disk1perusage	<Double>	Read-only	Used space in /var partition of the disk, as a percentage. This is a critical counter. You can configure /var Used (%) by using the Set snmp alarm DISK-USAGE-HIGH command.
disk0avail	<Double>	Read-only	Available space in /flash partition of the hard disk.
disk1avail	<Double>	Read-only	Available space in /var partition of the hard disk.
totrxmbits	<Double>	Read-only	Number of megabytes received by the Citrix ADC.
rxmbitsrate	<Double>	Read-only	Rate (/s) counter for totrxmbits
tottxmbits	<Double>	Read-only	Number of megabytes transmitted by the Citrix ADC.
txmbitsrate	<Double>	Read-only	Rate (/s) counter for tottxmbits
tcpcurclientconn	<Double>	Read-only	Client connections, including connections in the Opening, Established, and Closing state.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
tcpcurclientconnestablished	<Double>	Read-only	Current client connections in the Established state, which indicates that data transfer can occur between the Citrix ADC and the client.
tcpcurserverconn	<Double>	Read-only	Server connections, including connections in the Opening, Established, and Closing state.
tcpcurserverconnestablished	<Double>	Read-only	Current server connections in the Established state, which indicates that data transfer can occur between the Citrix ADC and the server.
httptotrequests	<Double>	Read-only	Total number of HTTP requests received.
httprequestsrate	<Double>	Read-only	Rate (/s) counter for httptotrequests
httptotresponses	<Double>	Read-only	Total number of HTTP responses sent.
httpresponsesrate	<Double>	Read-only	Rate (/s) counter for httptotresponses
httptotrxrequestbytes	<Double>	Read-only	Total number of bytes of HTTP

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			request data received.
httprxrequestbytesrate	<Double>	Read-only	Rate (/s) counter for httptotrxrequestbytes
httptotrxresponsebytes	<Double>	Read-only	Total number of bytes of HTTP response data received.
httprxresponsebytesrate	<Double>	Read-only	Rate (/s) counter for httptotrxresponsebytes
ssltottransactions	<Double>	Read-only	Number of SSL transactions on the Citrix ADC
ssltransactionsrate	<Double>	Read-only	Rate (/s) counter for ssltottransactions
ssltotsessionhits	<Double>	Read-only	Number of SSL session reuse hits on the Citrix ADC.
sslsessionhitsrate	<Double>	Read-only	Rate (/s) counter for ssltotsessionhits
appfirewallrequests	<Double>	Read-only	HTTP/HTTPS requests sent to your protected web servers via the Application Firewall.
appfirewallrequestsrate	<Double>	Read-only	Rate (/s) counter for appfirewallrequests
appfirewallresponses	<Double>	Read-only	HTTP/HTTPS responses sent by your protected web

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			servers via the Application Firewall.
appfirewallresponses rate	<Double>	Read-only	Rate (/s) counter for appfirewallresponses
appfirewallaborts	<Double>	Read-only	Incomplete HTTP/ HTTPS requests aborted by the client before the Application Firewall could finish processing them.
appfirewallabortsrate	<Double>	Read-only	Rate (/s) counter for appfirewallaborts
appfirewallredirects	<Double>	Read-only	HTTP/HTTPS requests redirected by the Application Firewall to a different Web page or web server. (HTTP 302)
appfirewallredirectsr ate	<Double>	Read-only	Rate (/s) counter for appfirewallredirects
enainbwlimitexceede d	<Double>	Read-only	Inbound BW Limits Exceeded
enainbwlimitexceede drate	<Double>	Read-only	Rate (/s) counter for enainbwlimitexceede d
enaoutbwlimitexceed ed	<Double>	Read-only	Outbound BW Limits Exceeded
enaoutbwlimitexceed edrate	<Double>	Read-only	Rate (/s) counter for enaoutbwlimitexceed ed

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
enappslimitexceeded	<Double>	Read-only	PPS Limits Exceeded
enappslimitexceeded rate	<Double>	Read-only	Rate (/s) counter for enappslimitexceeded
enaconntracklimitexceeded	<Double>	Read-only	Conn-Tracking Limits Exceeded
enaconntracklimitexceededrate	<Double>	Read-only	Rate (/s) counter for enaconntracklimitexceeded
enalinklocallimitexceeded	<Double>	Read-only	Link-Local Limits Exceeded
enalinklocallimitexceededrate	<Double>	Read-only	Rate (/s) counter for enalinklocallimitexceeded
enaconntracklimitavailable	<Double>	Read-only	Conn-Tracking Limits Available
enaconntracklimitavailablerate	<Double>	Read-only	Rate (/s) counter for enaconntracklimitavailable
misccounter0	<Double>	Read-only	Miscellaneous Counter 0.
misccounter1	<Double>	Read-only	Miscellaneous Counter 1.
numcpus	<Double>	Read-only	The number of CPUs on the Citrix ADC.

Operations

(click to see Properties)

- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/ns **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/ns? **args=detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get ns resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/ns? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

Note: To retrieve rate counters using attrs option, please provide parent counter name in attrs. e.g., to get "rxmbitsrate" attribute in the STAT response, attrs should be "totrxmbits"

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "ns": [ {

"appfirewallresponsesrate":<Double_value>,

"appfirewallredirects":<Double_value>,

"sslnumcardsup":<Double_value>,

"appfirewallrequests":<Double_value>,

"disk0avail":<Double_value>,

"rxmbitsrate":<Double_value>,

"httptotrxresponsebytes":<Double_value>,

"tcpcurserverconnestablished":<Double_value>,

"ssltotsessionhits":<Double_value>,

"cachetothits":<Double_value>,

"pktcpuusagepcnt":<Double_value>,

"cachetotmisses":<Double_value>,

"cachemaxmemorykb":<Double_value>,
```

```
"enaconntracklimitavailablerate":<Double_value>,

"starttimelocal":<String_value>,

"httprequestsrate":<Double_value>,

"disk1perusage":<Double_value>,

"appfirewallresponses":<Double_value>,

"cachepercentoriginbandwidthsaved":<Double_value>,

"appfirewallredirectsrate":<Double_value>,

"httprxresponsebytesrate":<Double_value>,

"enalinklocallimitexceeded":<Double_value>,

"enappslimitexceeded":<Double_value>,

"sslcards":<Double_value>,

"misccounter1":<Double_value>,

"hacurmasterstate":<String_value>,

"enalinklocallimitexceededrate":<Double_value>,

"memusagepcnt":<Double_value>,

"rescpuusage":<Double_value>,

"txmbitsrate":<Double_value>,

"httprxrequestbytesrate":<Double_value>,

"httpresponsesrate":<Double_value>,

"enaconntracklimitavailable":<Double_value>,

"compratio":<Double_value>,

"httptotresponses":<Double_value>,
```

```
"delcmpratio":<Double_value>,

"tcpcurserverconn":<Double_value>,

"hacurstate":<String_value>,

"enaconntracklimitexceeded":<Double_value>,

"cacheutilizedmemorykb":<Double_value>,

"cachemaxmemoryactivekb":<Double_value>,

"memuseinmb":<Double_value>,

"tcpcurclientconn":<Double_value>,

"mgmtcpuusagepcnt":<Double_value>,

"enappslimitexceededrate":<Double_value>,

"enaconntracklimitexceededrate":<Double_value>,

"ssltottransactions":<Double_value>,

"cpuusagepcnt":<Double_value>,

"cachemissesrate":<Double_value>,

"totrxmbits":<Double_value>,

"httptotrxrequestbytes":<Double_value>,

"appfirewallaborts":<Double_value>,

"starttime":<String_value>,

"ssltransactionsrate":<Double_value>,

"transtime":<String_value>,

"tcpcurclientconnestablished":<Double_value>,

"cpuusage":<Double_value>,
```

```
"enainbwlimitexceededrate":<Double_value>,

"appfirewallrequestsrate":<Double_value>,

"tottxmbits":<Double_value>,

"disk1avail":<Double_value>,

"cache64maxmemorykb":<Double_value>,

"enaoutbwlimitexceeded":<Double_value>,

"comptotaldatacompressionratio":<Double_value>,

"appfirewallabortsrate":<Double_value>,

"numcpus":<Double_value>,

"httptotrequests":<Double_value>,

"enainbwlimitexceeded":<Double_value>,

"resmemusage":<Double_value>,

"enaoutbwlimitexceededrate":<Double_value>,

"misccounter0":<Double_value>,

"sslsessionhitsrate":<Double_value>,

"cachehitsrate":<Double_value>,

"rescpuusagepcnt":<Double_value>,

"disk0perusage":<Double_value>

}]}
```

nsacl

Statistics for ACL entry resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
aclname	<String>	Read-write	Name of the extended ACL rule whose statistics you want the Citrix ADC to display. Minimum length = 1
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full
acltotpktsbridged	<Double>	Read-only	Packets matching a bridge ACL, which is in transparent mode and bypasses service processing.
aclpktsbridgedrate	<Double>	Read-only	Rate (/s) counter for acltotpktsbridged
acltotpktsdenied	<Double>	Read-only	Packets dropped because they match ACLs with processing mode set to DENY.
aclpktsdeniedrate	<Double>	Read-only	Rate (/s) counter for acltotpktsdenied
acltotpktsallowed	<Double>	Read-only	Packets matching ACLs with processing mode set to ALLOW. Citrix ADC processes these packets.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
aclpktsallowedrate	<Double>	Read-only	Rate (/s) counter for acltotpktsallowed
acltotpktsnat	<Double>	Read-only	Packets matching a NAT ACL, resulting in a NAT session.
aclpktsnatrate	<Double>	Read-only	Rate (/s) counter for acltotpktsnat
acltothits	<Double>	Read-only	Packets matching an ACL.
aclhitsrate	<Double>	Read-only	Rate (/s) counter for acltothits
acltotmisses	<Double>	Read-only	Packets not matching any ACL.
aclmissesrate	<Double>	Read-only	Rate (/s) counter for acltotmisses
acltotcount	<Double>	Read-only	Total number of ACL rules configured.
effectiveacltotcount	<Double>	Read-only	Total number of Effective ACL rules configured.
dfdacltothits	<Double>	Read-only	Packets matching an dfd ACL.
dfdaclhitsrate	<Double>	Read-only	Rate (/s) counter for dfdacltothits
dfdacltotmisses	<Double>	Read-only	Packets not matching any DFD ACL.
dfdaclmissesrate	<Double>	Read-only	Rate (/s) counter for dfdacltotmisses

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
dfdacltotcount	<Double>	Read-only	Total number of DFD ACL rules configured.
aclperhits	<Double>	Read-only	Number of times the acl was hit
aclperhitsrate	<Double>	Read-only	Rate (/s) counter for aclperhits

Operations

(click to see Properties)

- GET (ALL)
- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/nsacl **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/nsacl? **args=aclname: <String_value> ,detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get nsacl resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/nsacl? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "nsacl": [ {

"aclname":<String_value>,

"aclmissesrate":<Double_value>,

"aclpktsdeniedrate":<Double_value>,

"acltotmisses":<Double_value>,
```

```
"effectiveacltotcount":<Double_value>,

"aclperhits":<Double_value>,

"aclperhitsrate":<Double_value>,

"acltotpktsallowed":<Double_value>,

"acltotpktsbridged":<Double_value>,

"aclpktsallowedrate":<Double_value>,

"aclhitsrate":<Double_value>,

"dfdacltotmisses":<Double_value>,

"aclpktsnatrate":<Double_value>,

"acltotpktsnat":<Double_value>,

"dfdacltotcount":<Double_value>,

"acltothits":<Double_value>,

"dfdaclhitsrate":<Double_value>,

"dfdacltothits":<Double_value>,

"aclpktsbridgedrate":<Double_value>,

"acltotpktsdenied":<Double_value>,

"acltotcount":<Double_value>,

"dfdaclmissesrate":<Double_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/stat/nsacl/ aclname_value><String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "nsacl": [ {

"aclname":<String_value>,

"aclmissesrate":<Double_value>,

"aclpktsdeniedrate":<Double_value>,

"acltotmisses":<Double_value>,

"effectiveacltotcount":<Double_value>,

"aclperhits":<Double_value>,

"aclperhitsrate":<Double_value>,

"acltotpktsallowed":<Double_value>,

"acltotpktsbridged":<Double_value>,

"aclpktsallowedrate":<Double_value>,

"aclhitsrate":<Double_value>,

"dfdacltotmisses":<Double_value>,

"aclpktsnatrate":<Double_value>,
```

```
"acltotpktsnat":<Double_value>,

"dfdacltotcount":<Double_value>,

"acltothits":<Double_value>,

"dfdaclhitsrate":<Double_value>,

"dfdacltothits":<Double_value>,

"aclpktsbridgedrate":<Double_value>,

"acltotpktsdenied":<Double_value>,

"acltotcount":<Double_value>,

"dfdaclmissesrate":<Double_value>

}]}
```

nsacl6

Statistics for ACL6 entry resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
acl6name	<String>	Read-write	Name of the ACL6 rule whose statistics you want the Citrix ADC to display. Minimum length = 1
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
acl6totpktsbridged	<Double>	Read-only	Packets matching a bridge IPv6 ACL, which is in transparent mode and bypasses service processing.
acl6pktsbridgedrate	<Double>	Read-only	Rate (/s) counter for acl6totpktsbridged
acl6totpktsdenied	<Double>	Read-only	Packets dropped because they match IPv6 ACLs with processing mode set to DENY.
acl6pktsdeniedrate	<Double>	Read-only	Rate (/s) counter for acl6totpktsdenied
acl6totpktsallowed	<Double>	Read-only	Packets matching IPv6 ACLs with processing mode set to ALLOW. Citrix ADC processes these packets.
acl6pktsallowedrate	<Double>	Read-only	Rate (/s) counter for acl6totpktsallowed
acl6totpktsnat	<Double>	Read-only	Packets matching a NAT ACL6, resulting in a NAT session.
acl6pktsnatrate	<Double>	Read-only	Rate (/s) counter for acl6totpktsnat
acl6tothits	<Double>	Read-only	Packets matching an IPv6 ACL.
acl6hitsrate	<Double>	Read-only	Rate (/s) counter for acl6tothits

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
acl6totmisses	<Double>	Read-only	Packets not matching any IPv6 ACL.
acl6missesrate	<Double>	Read-only	Rate (/s) counter for acl6totmisses
acl6totpktsnat64	<Double>	Read-only	Packets matching a NAT64 ACL6, resulting in a NAT64 translation.
acl6pktsnat64rate	<Double>	Read-only	Rate (/s) counter for acl6totpktsnat64
acl6totcount	<Double>	Read-only	Total number of ACL6 rules configured.
dfdacl6totcount	<Double>	Read-only	Total number of DFD ACL6 rules configured.
dfdacl6tothits	<Double>	Read-only	Packets matching an dfd ACL6.
dfdacl6hitsrate	<Double>	Read-only	Rate (/s) counter for dfdacl6tothits
dfdacl6totmisses	<Double>	Read-only	Packets not matching any DFD ACL6.
dfdacl6missesrate	<Double>	Read-only	Rate (/s) counter for dfdacl6totmisses
acl6perhits	<Double>	Read-only	Number of times the acl6 was hit
acl6perhitsrate	<Double>	Read-only	Rate (/s) counter for acl6perhits

Operations

(click to see Properties)

- GET (ALL)
- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/nsacl6 **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/nsacl6? **args=acl6name: <String_value> ,detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get nsacl6 resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/nsacl6? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "nsacl6": [ {

"acl6name":<String_value>,

"acl6totpktsdenied":<Double_value>,

"acl6pktsbridgedrate":<Double_value>,

"dfdacl6hitsrate":<Double_value>,

"dfdacl6missesrate":<Double_value>,

"acl6missesrate":<Double_value>,

"acl6totcount":<Double_value>,

"acl6pktsnatrate":<Double_value>,

"acl6pktsallowedrate":<Double_value>,

"acl6perhits":<Double_value>,

"acl6totpktsnat64":<Double_value>,
```

```
"acl6tothits":<Double_value>,

"acl6totpktsnat":<Double_value>,

"acl6pktsdeniedrate":<Double_value>,

"acl6totpktsallowed":<Double_value>,

"acl6totmisses":<Double_value>,

"acl6perhitsrate":<Double_value>,

"dfdacl6totcount":<Double_value>,

"dfdacl6totmisses":<Double_value>,

"acl6pktsnat64rate":<Double_value>,

"acl6totpktsbridged":<Double_value>,

"dfdacl6tothits":<Double_value>,

"acl6hitsrate":<Double_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/stat/nsacl6/ acl6name_value><String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "nsacl6": [ {

"acl6name":<String_value>,

"acl6totpktsdenied":<Double_value>,

"acl6pktsbridgedrate":<Double_value>,

"dfdacl6hitsrate":<Double_value>,

"dfdacl6missesrate":<Double_value>,

"acl6missesrate":<Double_value>,

"acl6totcount":<Double_value>,

"acl6pktsnatrate":<Double_value>,

"acl6pktsallowedrate":<Double_value>,

"acl6perhits":<Double_value>,

"acl6totpktsnat64":<Double_value>,

"acl6tothits":<Double_value>,

"acl6totpktsnat":<Double_value>,

"acl6pktsdeniedrate":<Double_value>,

"acl6totpktsallowed":<Double_value>,

"acl6totmisses":<Double_value>,

"acl6perhitsrate":<Double_value>,

"dfdacl6totcount":<Double_value>,

"dfdacl6totmisses":<Double_value>,
```

```
"acl6pktsnat64rate":<Double_value>,

"acl6totpktsbridged":<Double_value>,

"dfdacl6tothits":<Double_value>,

"acl6hitsrate":<Double_value>

}]}
```

nslimitidentifier

Statistics for limit Identifier resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	The name of the identifier. Minimum length = 1
pattern	<String[]>	Read-write	Pattern for the selector field, ? means field is required, * means field value does not matter, anything else is a regular pattern.
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full
sortby	<String>	Read-write	use this argument to sort by specific key. Possible values = Hits

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
sortorder	<String>	Read-write	use this argument to specify sort order. Default value: SORT_DESCENDING Possible values = ascending, descending
ratelmtobjhits	<Double>	Read-only	Total hits.
ratelmtobjdrops	<Double>	Read-only	Total drops
ratelmtsessionobjhits	<Double>	Read-only	Total hits.

Operations

(click to see Properties)

- GET (ALL)
- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/nslimitidentifier **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/nslimitidentifier? **args=name: <String_value> ,pattern: <String_value> ,detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value> ,sortby: <String_value> ,sortorder: <String_value> ,sortorder: <String_value>**

Use this query-parameter to get nslimitidentifier resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/nslimitidentifier? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "nslimitidentifier": [ {

"name":<String_value>,

"ratelmtobjhits":<Double_value>,

"ratelmtobjdrops":<Double_value>,

"ratelmtsessionobjhits":<Double_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/stat/nslimitidentifier/ name_value><String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "nslimitidentifier": [ {

"name":<String_value>,

"ratelmtobjhits":<Double_value>,

"ratelmtobjdrops":<Double_value>,

"ratelmtsessionobjhits":<Double_value>
```

```
}]}
```

nsmemory

Statistics for resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
pool	<String>	Read-write	Feature name for which to display memory statistics. Minimum length = 1
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full
allocf	<Double>	Read-only	Memory allocation failure for particular feature.
memcurallocper	<Double>	Read-only	Percentage of Citrix ADC memory used by the feature.
memcurinkb	<Double>	Read-only	Total current Citrix ADC memory available for use by the feature, in kilobytes.

Operations

(click to see Properties)

- GET (ALL)
- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/nsmemory **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/nsmemory? **args=pool: <String_value> ,detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get nsmemory resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/nsmemory? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "nsmemory": [ {

"pool":<String_value>,

"memcurinkb":<Double_value>,

"allocf":<Double_value>,

"memcurallocper":<Double_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/stat/nsmemory/ pool_value><String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "nsmemory": [ {

"pool":<String_value>,

"memcurinkb":<Double_value>,

"allocf":<Double_value>,

"memcurallocper":<Double_value>

}]}
```

nspartition

Statistics for admin partition resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
partitionname	<String>	Read-write	Name of the partition. Minimum length = 1
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full
maxbandwidth	<Double>	Read-only	Maximum Banwidth allowed for the partition.
maxconnection	<Double>	Read-only	Maximum Connection allowed for the partition.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
maxmemory	<Double>	Read-only	Maximum memory limit for the partition.
currentbandwidth	<Double>	Read-only	Current Bandwidth usage for the partition.
currentconnections	<Double>	Read-only	Current Connections on this partition.
memoryusagepcnt	<Double>	Read-only	Memory usage(%) on this partition.
totaldrops	<Double>	Read-only	Total packet drops for the partition.
dropsrate	<Double>	Read-only	Rate (/s) counter for totaldrops
totaltokendrops	<Double>	Read-only	Total drops(KB) for the partition.
tokendropsrate	<Double>	Read-only	Rate (/s) counter for totaltokendrops
totalconnectiondrops	<Double>	Read-only	Total connection drops for the partition.
connectiondropsrate	<Double>	Read-only	Rate (/s) counter for totalconnectiondrops

Operations

(click to see Properties)

- GET (ALL)
- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/nspartition **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/nspartition? **args=partitionname: <String_value> ,detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get nspartition resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/nspartition? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "nspartition": [ {

"partitionname":<String_value>,

"totaltokendrops":<Double_value>,

"tokendropsrate":<Double_value>,

"totaldrops":<Double_value>,

"maxbandwidth":<Double_value>,

"maxconnection":<Double_value>,

"connectiondropsrate":<Double_value>,

"currentconnections":<Double_value>,

"totalconnectiondrops":<Double_value>,

"maxmemory":<Double_value>,

"dropsrate":<Double_value>,

"memoryusagepcnt":<Double_value>,

"currentbandwidth":<Double_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/stat/nspartition/ partitionname_value><String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "nspartition": [ {

"partitionname":<String_value>,

"totaltokendrops":<Double_value>,

"tokendropsrate":<Double_value>,

"totaldrops":<Double_value>,

"maxbandwidth":<Double_value>,

"maxconnection":<Double_value>,

"connectiondropsrate":<Double_value>,

"currentconnections":<Double_value>,

"totalconnectiondrops":<Double_value>,

"maxmemory":<Double_value>,

"dropsrate":<Double_value>,
```

```
"memoryusagepcnt":<Double_value>,

"currentbandwidth":<Double_value>

}]}
```

nspbr

Statistics for Policy Based Routing(PBR) entry resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the PBR whose statistics you want the Citrix ADC to display. Minimum length = 1
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full
pbrtotpktsallowed	<Double>	Read-only	Total packets that matched the PBR (Policy-Based Routes) with action ALLOW
pbrpktsallowedrate	<Double>	Read-only	Rate (/s) counter for pbrtotpktsallowed
pbrtotpktsdenied	<Double>	Read-only	Total packets that matched the PBR with action DENY

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
pbrpktsdeniedrate	<Double>	Read-only	Rate (/s) counter for pbrtotpktsdenied
pbrtothits	<Double>	Read-only	Total packets that matched one of the configured PBR
pbrhitsrate	<Double>	Read-only	Rate (/s) counter for pbrtothits
pbrtotmisses	<Double>	Read-only	Total packets that did not match any PBR
pbrmissesrate	<Double>	Read-only	Rate (/s) counter for pbrtotmisses
pbrtotnulldrop	<Double>	Read-only	Total packets that are dropped due to null nexthop
pbrnulldroprate	<Double>	Read-only	Rate (/s) counter for pbrtotnulldrop
pbrcount	<Double>	Read-only	Total Number of PBR
pbreffectivecount	<Double>	Read-only	Total Number of Effective PBR
pbrperhits	<Double>	Read-only	Number of times the pbr was hit
pbrperhitsrate	<Double>	Read-only	Rate (/s) counter for pbrperhits

Operations

(click to see Properties)

- GET (ALL)
- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/nspbr **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/nspbr? **args=name: <String_value> ,detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get nspbr resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/nspbr? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "nspbr": [ {

"name":<String_value>,

"pbrperhits":<Double_value>,

"pbrtotnulldrop":<Double_value>,

"pbrtotmisses":<Double_value>,

"pbrpktsdeniedrate":<Double_value>,

"pbrmissesrate":<Double_value>,

"pbrnulldroprate":<Double_value>,

"pbrcount":<Double_value>,

"pbrtotpktsdenied":<Double_value>,

"pbreffectivecount":<Double_value>,

"pbrtothits":<Double_value>,

"pbrhitsrate":<Double_value>,

"pbrpktsallowedrate":<Double_value>,

"pbrperhitsrate":<Double_value>,

"pbrtotpktsallowed":<Double_value>
```

```
}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/stat/nspbr/ name_value><String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "nspbr": [ {

"name":<String_value>,

"pbrperhits":<Double_value>,

"pbrtotnulldrop":<Double_value>,

"pbrtotmisses":<Double_value>,

"pbrpktsdeniedrate":<Double_value>,

"pbrmissesrate":<Double_value>,

"pbrnulldroprate":<Double_value>,

"pbrcount":<Double_value>,

"pbrtotpktsdenied":<Double_value>,
```

```
"pbreffectivecount":<Double_value>,

"pbrtothits":<Double_value>,

"pbrhitsrate":<Double_value>,

"pbrpktsallowedrate":<Double_value>,

"pbrperhitsrate":<Double_value>,

"pbrtotpktsallowed":<Double_value>

}]}
```

nspbr6

Statistics for PBR6 entry resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the PBR6 whose statistics you want the Citrix ADC to display. Minimum length = 1
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full
pbr6totpktsallowed	<Double>	Read-only	Total packets that matched the PBR6 with action ALLOW
pbr6pktsallowedrate	<Double>	Read-only	Rate (/s) counter for pbr6totpktsallowed

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
pbr6totpktsdenied	<Double>	Read-only	Total packets that matched PBR6 with action DENY
pbr6pktsdeniedrate	<Double>	Read-only	Rate (/s) counter for pbr6totpktsdenied
pbr6tothits	<Double>	Read-only	Total packets that matched one of the configured PBR6
pbr6hitsrate	<Double>	Read-only	Rate (/s) counter for pbr6tothits
pbr6totmisses	<Double>	Read-only	Total packets that did not match any PBR6
pbr6missesrate	<Double>	Read-only	Rate (/s) counter for pbr6totmisses
pbr6totnulldrop	<Double>	Read-only	Total packets that are dropped due to null next hop
pbr6nulldroprate	<Double>	Read-only	Rate (/s) counter for pbr6totnulldrop
pbr6perhits	<Double>	Read-only	Number of times the pbr6 was hit
pbr6perhitsrate	<Double>	Read-only	Rate (/s) counter for pbr6perhits

Operations

(click to see Properties)

- GET (ALL)
- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/nspbr6 **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/nspbr6? **args=name: <String_value> ,detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get nspbr6 resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/nspbr6? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "nspbr6": [ {

"name":<String_value>,

"pbr6hitsrate":<Double_value>,

"pbr6perhitsrate":<Double_value>,

"pbr6nulldroprate":<Double_value>,

"pbr6totmisses":<Double_value>,

"pbr6pktsdeniedrate":<Double_value>,

"pbr6totpktsallowed":<Double_value>,

"pbr6totnulldrop":<Double_value>,

"pbr6perhits":<Double_value>,

"pbr6tothits":<Double_value>,

"pbr6pktsallowedrate":<Double_value>,

"pbr6totpktsdenied":<Double_value>,

"pbr6missesrate":<Double_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/stat/nspbr6/ name_value><String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "nspbr6": [ {

"name":<String_value>,

"pbr6hitsrate":<Double_value>,

"pbr6perhitsrate":<Double_value>,

"pbr6nulldroprate":<Double_value>,

"pbr6totmisses":<Double_value>,

"pbr6pktsdeniedrate":<Double_value>,

"pbr6totpktsallowed":<Double_value>,

"pbr6totnulldrop":<Double_value>,

"pbr6perhits":<Double_value>,

"pbr6tothits":<Double_value>,

"pbr6pktsallowedrate":<Double_value>,
```

```
"pbr6totpktsdenied":<Double_value>,

"pbr6missesrate":<Double_value>

}]}
```

nssimpleacl

Statistics for simple ACL resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full
sacltothits	<Double>	Read-only	Packets matching a SimpleACL.
saclhitsrate	<Double>	Read-only	Rate (/s) counter for sacltothits
sacltotmisses	<Double>	Read-only	Packets not matching any SimpleACL.
saclmissesrate	<Double>	Read-only	Rate (/s) counter for sacltotmisses
saclscount	<Double>	Read-only	Number of SimpleACLs configured.
sacltotpktsallowed	<Double>	Read-only	Total packets that matched a SimpleACL with action ALLOW and

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			got consumed by Citrix ADC.
saclpktsallowedrate	<Double>	Read-only	Rate (/s) counter for sacltotpktsallowed
sacltotpktsbridged	<Double>	Read-only	Total packets that matched a SimpleACL with action BRIDGE and got bridged by Citrix ADC.
saclpktsbridgedrate	<Double>	Read-only	Rate (/s) counter for sacltotpktsbridged
sacltotpktsdenied	<Double>	Read-only	Packets dropped because they match SimpleACL (Access Control List) with processing mode set to DENY.
saclpktsdeniedrate	<Double>	Read-only	Rate (/s) counter for sacltotpktsdenied

Operations

(click to see Properties)

- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/nssimpleacl **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/nssimpleacl? **args=detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get nssimpleacl resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/nssimpleacl? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "nssimpleacl": [ {

"sacltotpktsbridged":<Double_value>,

"saclhitsrate":<Double_value>,

"saclmissesrate":<Double_value>,

"sacltotpktsdenied":<Double_value>,

"saclpktsbridgedrate":<Double_value>,

"saclpktsallowedrate":<Double_value>,

"saclscount":<Double_value>,

"sacltothits":<Double_value>,

"sacltotmisses":<Double_value>,

"saclpktsdeniedrate":<Double_value>,

"sacltotpktsallowed":<Double_value>

}]}
```

nssimpleacl6

Statistics for simple ACL6 resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
clearstats	<String>	Read-write	Clear the statsistics / counters.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = basic, full
sacl6tothits	<Double>	Read-only	Packets matching a SimpleACL6.
sacl6hitsrate	<Double>	Read-only	Rate (/s) counter for sacl6tothits
sacl6totmisses	<Double>	Read-only	Packets not matching any SimpleACL6.
sacl6missesrate	<Double>	Read-only	Rate (/s) counter for sacl6totmisses
sacl6scount	<Double>	Read-only	Number of SimpleACL6s configured.
sacl6totpktsallowed	<Double>	Read-only	Total packets that matched a SimpleACL6 with action ALLOW and got consumed by Citrix ADC.
sacl6pktsallowedrate	<Double>	Read-only	Rate (/s) counter for sacl6totpktsallowed
sacl6totpktsbridged	<Double>	Read-only	Total packets that matched a SimpleACL6 with action BRIDGE and got bridged by Citrix ADC.
sacl6pktsbridgedrate	<Double>	Read-only	Rate (/s) counter for sacl6totpktsbridged

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
sacl6totpktsdenied	<Double>	Read-only	Packets dropped because they match SimpleACL6 with processing mode set to DENY.
sacl6pktsdeniedrate	<Double>	Read-only	Rate (/s) counter for sacl6totpktsdenied

Operations

(click to see Properties)

- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/nssimpleacl6 **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/nssimpleacl6? **args=detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get nssimpleacl6 resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/nssimpleacl6? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "nssimpleacl6": [ {

"sacl6missesrate":<Double_value>,

"sacl6pktsbridgedrate":<Double_value>,

"sacl6pktsallowedrate":<Double_value>,

"sacl6totpktsallowed":<Double_value>,

"sacl6totpktsbridged":<Double_value>,
```

```
"sacl6pktsdeniedrate":<Double_value>,

"sacl6hitsrate":<Double_value>,

"sacl6tothits":<Double_value>,

"sacl6totmisses":<Double_value>,

"sacl6scount":<Double_value>,

"sacl6totpktsdenied":<Double_value>

}]}
```

nstrafficdomain

Statistics for Traffic Domain resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
td	<Integer>	Read-write	An integer specifying the Traffic Domain ID. Possible values: 1 through 4094. Minimum value = 1 Maximum value = 4094
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full
nstdtotrxpkts	<Double>	Read-only	Packets received on this TD.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
nstdrxpktsrate	<Double>	Read-only	Rate (/s) counter for nstdtotrxpkts
nstdtottxpkts	<Double>	Read-only	Packets transmitted from this TD.
nstdtxpktsrate	<Double>	Read-only	Rate (/s) counter for nstdtottxpkts
nstdtotdroppedpkts	<Double>	Read-only	Inbound packets dropped on this TD by reception.
nstddroppedpktsrate	<Double>	Read-only	Rate (/s) counter for nstdtotdroppedpkts

Operations

(click to see Properties)

- GET (ALL)
- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/nstrafficdomain **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/nstrafficdomain? **args=td: <Integer_value> ,detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get nstrafficdomain resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/nstrafficdomain? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "nstrafficdomain": [ {

"td":<Integer_value>,
```

```
"nstdtxpktsrate":<Double_value>,

"nstdtotdroppedpkts":<Double_value>,

"nstdrxpktsrate":<Double_value>,

"nstddroppedpktsrate":<Double_value>,

"nstdtotrxpkts":<Double_value>,

"nstdtottxpkts":<Double_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/stat/nstrafficdomain/ td_value><Integer> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "nstrafficdomain": [ {

"td":<Integer_value>,

"nstdtxpktsrate":<Double_value>,

"nstdtotdroppedpkts":<Double_value>,
```

```
"nstdrxpktsrate":<Double_value>,

"nstddroppedpktsrate":<Double_value>,

"nstdtotrxpkts":<Double_value>,

"nstdtottxpkts":<Double_value>

}]}
```

pcp

Pcp

Port Control Protocol statistics.

NAME	DESCRIPTION
pcpserver	Statistics for server resource.

pcpserver

Statistics for server resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	PCP Statistics per Server.
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full
pcptotrequests	<Double>	Read-only	PCP Request received.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
pcprequestsrate	<Double>	Read-only	Rate (/s) counter for pcptotrequests
pcptotresponses	<Double>	Read-only	Number PCP responces sent.
pcpresponsesrate	<Double>	Read-only	Rate (/s) counter for pcptotresponses
pcptotmaprequests	<Double>	Read-only	PCP MAP Requests received.
pcpmaprequestsrate	<Double>	Read-only	Rate (/s) counter for pcptotmaprequests
pcptotpeerrequests	<Double>	Read-only	PCP PEER Requests received.
pcppeerrequestsrate	<Double>	Read-only	Rate (/s) counter for pcptotpeerrequests
pcptoterrinrquest	<Double>	Read-only	total PCP request with error.
pcperrinrquestrate	<Double>	Read-only	Rate (/s) counter for pcptoterrinrquest
pcptoterrinres	<Double>	Read-only	Total PCP responses with errors.
pcperrinresrate	<Double>	Read-only	Rate (/s) counter for pcptoterrinres
pcptotunsuppvers	<Double>	Read-only	PCP request with unsupported version.
pcpunsuppversrate	<Double>	Read-only	Rate (/s) counter for pcptotunsuppvers
pcptotmalformedreq	<Double>	Read-only	total PCP request having malformed PCP packets.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
pcpmalformedreqrate	<Double>	Read-only	Rate (/s) counter for pcptotmalformedreq
pcptotunsuppopcode	<Double>	Read-only	total Unsupproted OPCODES received Requests.
pcpunsuppopcoderate	<Double>	Read-only	Rate (/s) counter for pcptotunsuppopcode
pcptotunsuppoption	<Double>	Read-only	total Unsupproted OPTIONS received in requests.
pcpunsuppoptionrate	<Double>	Read-only	Rate (/s) counter for pcptotunsuppoption
pcptotmalformedoption	<Double>	Read-only	total malformed OPTIONS received in requests.
pcpmalformedoptionrate	<Double>	Read-only	Rate (/s) counter for pcptotmalformedoption
pcptotnetfailure	<Double>	Read-only	Total Network Failures.
pcpnetfailurerate	<Double>	Read-only	Rate (/s) counter for pcptotnetfailure
pcptotnoresources	<Double>	Read-only	no resources
pcpnoresourcesrate	<Double>	Read-only	Rate (/s) counter for pcptotnoresources
pcptotunsupportedprotocol	<Double>	Read-only	Total Unsupported Protocols requests.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
pcpunsupportedprotocolrate	<Double>	Read-only	Rate (/s) counter for pcptotunsupportedprotocol
pcptotuserexqouta	<Double>	Read-only	Total user ex quota.
pcpuserexqoutarate	<Double>	Read-only	Rate (/s) counter for pcptotuserexqouta
pcptotnoexternal	<Double>	Read-only	Total responses with opcode can not provide external.
pcpnoexternalrate	<Double>	Read-only	Rate (/s) counter for pcptotnoexternal
pcptotaddrmismatch	<Double>	Read-only	Total address mismatch.
pcpaddrmismatchrate	<Double>	Read-only	Rate (/s) counter for pcptotaddrmismatch
pcptotexcesspeers	<Double>	Read-only	Total responses with opcode excessive remote peers.
pcpexcesspeersrate	<Double>	Read-only	Rate (/s) counter for pcptotexcesspeers

Operations

(click to see Properties)

- GET (ALL)
- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/pcpserver **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/pcpserver? **args=name: <String_value> ,detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get pcpserver resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/pcpserver? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "pcpserver": [ {

"name":<String_value>,

"pcptotrequests":<Double_value>,

"pcpmalformedoptionrate":<Double_value>,

"pcpunsuppversrate":<Double_value>,

"pcpmalformedreqrate":<Double_value>,

"pcptotunsuppvers":<Double_value>,

"pcptotmalformedoption":<Double_value>,

"pcptotpeerrequests":<Double_value>,

"pcpaddrmismatchrate":<Double_value>,

"pcptotnetfailure":<Double_value>,

"pcpunsuppoptionrate":<Double_value>,

"pcptotmaprequests":<Double_value>,

"pcpnoexternalrate":<Double_value>,

"pcptotuserexqouta":<Double_value>,

"pcpnetfailurerate":<Double_value>,

"pcperrinrquestrate":<Double_value>,
```

```
"pcptotunsuppoption":<Double_value>,

"pcpunsuppopcoderate":<Double_value>,

"pcptotexcesspeers":<Double_value>,

"pcptoterrinrquest":<Double_value>,

"pcpnoresourcesrate":<Double_value>,

"pcptotnoexternal":<Double_value>,

"pcpunsupportedprotocolrate":<Double_value>,

"pcptotaddrmismatch":<Double_value>,

"pcprequestsrate":<Double_value>,

"pcptoterrinres":<Double_value>,

"pcppeerrequestsrate":<Double_value>,

"pcptotmalformedreq":<Double_value>,

"pcptotunsupportedprotocol":<Double_value>,

"pcpexcesspeersrate":<Double_value>,

"pcptotresponses":<Double_value>,

"pcpmaprequestsrate":<Double_value>,

"pcptotnoresources":<Double_value>,

"pcpuserexqoutarate":<Double_value>,

"pcptotunsuppopcode":<Double_value>,

"pcperrinresrate":<Double_value>,

"pcpresponsesrate":<Double_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/stat/pcpserver/ name_value><String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "pcpserver": [ {

"name":<String_value>,

"pcptotrequests":<Double_value>,

"pcpmalformedoptionrate":<Double_value>,

"pcpunsuppversrate":<Double_value>,

"pcpmalformedreqrate":<Double_value>,

"pcptotunsuppvers":<Double_value>,

"pcptotmalformedoption":<Double_value>,

"pcptotpeerrequests":<Double_value>,

"pcpaddrmismatchrate":<Double_value>,

"pcptotnetfailure":<Double_value>,
```

```
"pcpunsuppoptionrate":<Double_value>,

"pcptotmaprequests":<Double_value>,

"pcpnoexternalrate":<Double_value>,

"pcptotuserexqouta":<Double_value>,

"pcpnetfailurerate":<Double_value>,

"pcperrinrquestrate":<Double_value>,

"pcptotunsuppoption":<Double_value>,

"pcpunsuppopcoderate":<Double_value>,

"pcptotexcesspeers":<Double_value>,

"pcptoterrinrquest":<Double_value>,

"pcpnoresourcesrate":<Double_value>,

"pcptotnoexternal":<Double_value>,

"pcpunsupportedprotocolrate":<Double_value>,

"pcptotaddrmismatch":<Double_value>,

"pcprequestsrate":<Double_value>,

"pcptoterrinres":<Double_value>,

"pcppeerrequestsrate":<Double_value>,

"pcptotmalformedreq":<Double_value>,

"pcptotunsupportedprotocol":<Double_value>,

"pcpexcesspeersrate":<Double_value>,

"pcptotresponses":<Double_value>,

"pcpmaprequestsrate":<Double_value>,
```

```
"pcptotnoresources":<Double_value>,

"pcpuserexqoutarate":<Double_value>,

"pcptotunsuppopcode":<Double_value>,

"pcperrinresrate":<Double_value>,

"pcpresponsesrate":<Double_value>

}]}
```

protocol

Protocol

Protocol statistics.

NAME	DESCRIPTION
protocolhttp	Statistics for HTTP resource.
protocolhttp2	Statistics for http2 resource.
protocolhttp3	Statistics for http3 resource.
protocolicmp	Statistics for icmp resource.
protocolicmpv6	Statistics for icmpv6 resource.
protocolip	Statistics for protocolip resource.
protocolipv6	Statistics for ip v6 resource.
protocolmptcp	Statistics for mptcp protocol resource.

NAME	DESCRIPTION
protocolquic	Statistics for QUIC protocol resource.
protocolquicbridge	Statistics for QUIC Bridge protocol resource.
protocoltcp	Statistics for tcp protocol resource.
protocoludp	Statistics for UDP Protocol resource.

protocolhttp

Statistics for HTTP resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full
httptotrequests	<Double>	Read-only	Total number of HTTP requests received.
httprequestsrate	<Double>	Read-only	Rate (/s) counter for httptotrequests
httptotresponses	<Double>	Read-only	Total number of HTTP responses sent.
httpresponsesrate	<Double>	Read-only	Rate (/s) counter for httptotresponses

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
httptotrxrequestbytes	<Double>	Read-only	Total number of bytes of HTTP request data received.
httprxrequestbytesrate	<Double>	Read-only	Rate (/s) counter for httptotrxrequestbytes
httptotrxresponsebytes	<Double>	Read-only	Total number of bytes of HTTP response data received.
httprxresponsebytesrate	<Double>	Read-only	Rate (/s) counter for httptotrxresponsebytes
httptotgets	<Double>	Read-only	Total number of HTTP requests received with the GET method.
httpgetsrate	<Double>	Read-only	Rate (/s) counter for httptotgets
httptotposts	<Double>	Read-only	Total number of HTTP requests received with the POST method.
httppostsrate	<Double>	Read-only	Rate (/s) counter for httptotposts
httptotothers	<Double>	Read-only	Total number of HTTP requests received with methods other than GET and POST. Some of the other well-defined HTTP methods are HEAD,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			PUT, DELETE, OPTIONS, and TRACE. User-defined methods are also allowed.
httptohersrate	<Double>	Read-only	Rate (/s) counter for httptotothers
httptot10requests	<Double>	Read-only	Total number of HTTP/1.0 requests received.
http10requestsrate	<Double>	Read-only	Rate (/s) counter for httptot10requests
httptot11requests	<Double>	Read-only	Total number of HTTP/1.1 requests received.
http11requestsrate	<Double>	Read-only	Rate (/s) counter for httptot11requests
httptotclenrequests	<Double>	Read-only	Total number of HTTP requests in which the Content-length field of the HTTP header has been set. Content-length specifies the length of the content, in bytes, in the associated HTTP body.
httpclenrequestsrate	<Double>	Read-only	Rate (/s) counter for httptotclenrequests
httptotchunkedrequests	<Double>	Read-only	Total number of HTTP requests in which the Transfer-Encoding field of the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			HTTP header has been set to chunked.
httpchunkedrequestsrate	<Double>	Read-only	Rate (/s) counter for httptotchunkedrequests
httptottxrequestbytes	<Double>	Read-only	Total number of bytes of HTTP request data transmitted.
httptxrequestbytesrate	<Double>	Read-only	Rate (/s) counter for httptottxrequestbytes
httptot10responses	<Double>	Read-only	Total number of HTTP/1.0 responses sent.
http10responsesrate	<Double>	Read-only	Rate (/s) counter for httptot10responses
httptot11responses	<Double>	Read-only	Total number of HTTP/1.1 responses sent.
http11responsesrate	<Double>	Read-only	Rate (/s) counter for httptot11responses
httptotclenresponses	<Double>	Read-only	Total number of HTTP responses sent in which the Content-length field of the HTTP header has been set. Content-length specifies the length of the content, in bytes, in the associated HTTP body.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
httpclenresponsesrate	<Double>	Read-only	Rate (/s) counter for httptotclenresponses
httptotchunkedresponses	<Double>	Read-only	Total number of HTTP responses sent in which the Transfer-Encoding field of the HTTP header has been set to chunked. This setting is used when the server wants to start sending the response before knowing its total length. The server breaks the response into chunks and sends them in sequence, inserting the length of each chunk before the actual data. The message ends with a chunk of size zero.
httpchunkedresponsesrate	<Double>	Read-only	Rate (/s) counter for httptotchunkedresponses
httperrnoreusemultipart	<Double>	Read-only	Total number of HTTP multi-part responses sent. In multi-part responses, one or more entities are encapsulated within the body of a single message.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
httperrnoreusemultipartrate	<Double>	Read-only	Rate (/s) counter for httperrnoreusemultipart
httptotnoclenchunkresponses	<Double>	Read-only	Total number of FIN-terminated responses sent. In FIN-terminated responses, the server finishes sending the data and closes the connection.
httpnoclenchunkresponsesrate	<Double>	Read-only	Rate (/s) counter for httptotnoclenchunkresponses
httptottxresponsebytes	<Double>	Read-only	Total number of bytes of HTTP response data transmitted.
httptxresponsebytesrate	<Double>	Read-only	Rate (/s) counter for httptottxresponsebytes
httperrincompleteheaders	<Double>	Read-only	Total number of HTTP requests and responses received in which the HTTP header spans more than one packet.
httperrincompletereq uests	<Double>	Read-only	Total number of HTTP requests received in which the header spans more than one packet.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
httperrincompletereq uestsrate	<Double>	Read-only	Rate (/s) counter for httperrincompletereq uests
httperrincompleteres ponses	<Double>	Read-only	Total number of HTTP responses received in which the header spans more than one packet.
httperrincompleteres ponsesrate	<Double>	Read-only	Rate (/s) counter for httperrincompleteres ponses
httperrserverbusy	<Double>	Read-only	Total number of HTTP error responses received. Some of the error responses are: 500 Internal Server Error 501 Not Implemented 502 Bad Gateway 503 Service Unavailable 504 Gateway Timeout 505 HTTP Version Not Supported
httperrserverbusyrat e	<Double>	Read-only	Rate (/s) counter for httperrserverbusy
httperrlargecontent	<Double>	Read-only	Total number of requests and responses received with large body.
httperrlargechunk	<Double>	Read-only	Total number of requests received with large chunk size, in which the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Transfer-Encoding field of the HTTP header has been set to chunked.
httperrlargectlen	<Double>	Read-only	Total number of requests received with large content, in which the Content-length field of the HTTP header has been set. Content-length specifies the length of the content, in bytes, in the associated HTTP body.
httperrrfc7230desyncctlente	<Double>	Read-only	Total number of requests/responses received with both content-length and transfer encoding headers - RFC7230 Non-compliance
httperrrfc7230desynmultictlen	<Double>	Read-only	Total number of request/response received with multiple content-length headers with different values - RFC7230 Non-compliance
httperrrfc7230desynidenticalctlen	<Double>	Read-only	Total number of request/response received with duplicate content-length headers -

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			RFC7230 Non-compliance
httperrinvalidhostheader	<Double>	Read-only	Total number of request received with invalid host header

Operations

(click to see Properties)

- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/protocolhttp **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/protocolhttp? **args=detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get protocolhttp resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/protocolhttp? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "protocolhttp": [ {

"http11requestsrate":<Double_value>,

"httptotclenresponses":<Double_value>,

"httptohersrate":<Double_value>,

"httptotrxresponsebytes":<Double_value>,

"httpchunkedresponsesrate":<Double_value>,
```

```
"http11responsesrate":<Double_value>,

"httperrserverbusyrate":<Double_value>,

"httprequestsrate":<Double_value>,

"httptotchunkedrequests":<Double_value>,

"httptotchunkedresponses":<Double_value>,

"httptotgets":<Double_value>,

"httptotclenrequests":<Double_value>,

"httptotnoclenchunkresponses":<Double_value>,

"httperrlargectlen":<Double_value>,

"httperrinvalidhostheader":<Double_value>,

"httprxrequestbytesrate":<Double_value>,

"httperrserverbusy":<Double_value>,

"httppostsrate":<Double_value>,

"httptottxresponsebytes":<Double_value>,

"httprxresponsebytesrate":<Double_value>,

"httperrincompleterequests":<Double_value>,

"httperrincompleterequestsrate":<Double_value>,

"httptxrequestbytesrate":<Double_value>,

"httptotresponses":<Double_value>,

"httpresponsesrate":<Double_value>,

"httptxresponsebytesrate":<Double_value>,

"httptotposts":<Double_value>,
```

```
"httperrrfc7230desynidenticalctlen":<Double_value>,

"httptot11requests":<Double_value>,

"httperrincompleteheaders":<Double_value>,

"httperrrfc7230desynmultictlen":<Double_value>,

"httptot11responses":<Double_value>,

"httptot10responses":<Double_value>,

"httperrincompleteresponsesrate":<Double_value>,

"httpnoclenchunkresponsesrate":<Double_value>,

"httptotothers":<Double_value>,

"httptot10requests":<Double_value>,

"httptotrxrequestbytes":<Double_value>,

"httpgetsrate":<Double_value>,

"httpchunkedrequestsrate":<Double_value>,

"httpclenresponsesrate":<Double_value>,

"httperrlargechunk":<Double_value>,

"httpclenrequestsrate":<Double_value>,

"http10responsesrate":<Double_value>,

"httperrnoreusemultipart":<Double_value>,

"httperrlargecontent":<Double_value>,

"httperrnoreusemultipartrate":<Double_value>,

"http10requestsrate":<Double_value>,

"httperrrfc7230desynctlente":<Double_value>,
```

```
"httptotrequests":<Double_value>,

"httperrincompleteresponses":<Double_value>,

"httptottxrequestbytes":<Double_value>

}]}
```

protocolhttp2

Statistics for http2 resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full
http2requests	<Double>	Read-only	Total number of http2 requests
http2requestsrate	<Double>	Read-only	Rate (/s) counter for http2requests
http2responses	<Double>	Read-only	Total number of http2 responses
http2responsesrate	<Double>	Read-only	Rate (/s) counter for http2responses
http2totgrpcrequest	<Double>	Read-only	Total number of gRPC requests
http2grpcrequestrate	<Double>	Read-only	Rate (/s) counter for http2totgrpcrequest

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
http2totgrpcresponse	<Double>	Read-only	Total number of gRPC responses
http2grpcresponserate	<Double>	Read-only	Rate (/s) counter for http2totgrpcresponse
http2totgrpcsuccess	<Double>	Read-only	Total number of gRPC success
http2grpcsuccessrate	<Double>	Read-only	Rate (/s) counter for http2totgrpcsuccess
http2totgrpcfailure	<Double>	Read-only	Total number of gRPC failures
http2grpcfailurerate	<Double>	Read-only	Rate (/s) counter for http2totgrpcfailure
http2direct	<Double>	Read-only	Total number of http2 direct connections established
http2directrate	<Double>	Read-only	Rate (/s) counter for http2direct
http2serverdirect	<Double>	Read-only	Number of HTTP/2 server direct
http2serverdirectrate	<Double>	Read-only	Rate (/s) counter for http2serverdirect
http2requpg	<Double>	Read-only	Total number of connections upgraded to HTTP2
http2requpgrate	<Double>	Read-only	Rate (/s) counter for http2requpg
http2nomatcipher	<Double>	Read-only	Total number of cipher mismatch failures

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
http2nomatcipherrate	<Double>	Read-only	Rate (/s) counter for http2nomatcipher
http2serverdirectfailed	<Double>	Read-only	Number of HTTP/2 server direct failed
http2serverdirectfailedrate	<Double>	Read-only	Rate (/s) counter for http2serverdirectfailed
http2serverupgradefailed	<Double>	Read-only	Number of HTTP/2 server upgrade failed
http2serverupgradefailedrate	<Double>	Read-only	Rate (/s) counter for http2serverupgradefailed
http2requestupgradefailed	<Double>	Read-only	Number of HTTP/2 request upgrade failed
http2requestupgradefailedrate	<Double>	Read-only	Rate (/s) counter for http2requestupgradefailed
http2dataframessent	<Double>	Read-only	Number of HTTP/2 DATA frames sent
http2dataframessentrate	<Double>	Read-only	Rate (/s) counter for http2dataframessent
http2headerframessent	<Double>	Read-only	Number of HTTP/2 HEADER frames sent
http2headerframessentrate	<Double>	Read-only	Rate (/s) counter for http2headerframessent

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
http2priorityframessent	<Double>	Read-only	Number of HTTP/2 PRIORITY frames sent
http2priorityframessentrate	<Double>	Read-only	Rate (/s) counter for http2priorityframessent
http2rststreamframessent	<Double>	Read-only	Number of HTTP/2 RST_STREAM frames sent
http2rststreamframessentrate	<Double>	Read-only	Rate (/s) counter for http2rststreamframessent
http2settingframessent	<Double>	Read-only	Number of HTTP/2 SETTINGS frames sent
http2settingframessentrate	<Double>	Read-only	Rate (/s) counter for http2settingframessent
http2pushpromiseframessent	<Double>	Read-only	Number of HTTP/2 PUSH_PROMISE frames sent
http2pushpromiseframessentrate	<Double>	Read-only	Rate (/s) counter for http2pushpromiseframessent
http2pingframessent	<Double>	Read-only	Number of HTTP/2 PING frames sent
http2pingframessentrate	<Double>	Read-only	Rate (/s) counter for http2pingframessent
http2goawayframessent	<Double>	Read-only	Number of HTTP/2 GOAWAY frames sent

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
http2goawayframessentrate	<Double>	Read-only	Rate (/s) counter for http2goawayframessent
http2windowupdateframessent	<Double>	Read-only	Number of HTTP/2 WINDOW_UPDATE frames sent
http2windowupdateframessentrate	<Double>	Read-only	Rate (/s) counter for http2windowupdateframessent
http2continuationframessent	<Double>	Read-only	Number of HTTP/2 CONTINUATION frames sent
http2continuationframessentrate	<Double>	Read-only	Rate (/s) counter for http2continuationframessent
http2altsvcframessent	<Double>	Read-only	Number of HTTP/2 ALTSVC frames sent
http2altsvcframessentrate	<Double>	Read-only	Rate (/s) counter for http2altsvcframessent
http2dataframesrcvd	<Double>	Read-only	Number of HTTP/2 DATA frames received
http2dataframesrcvdrate	<Double>	Read-only	Rate (/s) counter for http2dataframesrcvd
http2headerframesrcvd	<Double>	Read-only	Total number of http2 header frames received
http2headerframesrcvdrate	<Double>	Read-only	Rate (/s) counter for http2headerframesrcvd

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
http2priorityframesrcvd	<Double>	Read-only	Total number of http2 priority frames received
http2priorityframesrcvdrate	<Double>	Read-only	Rate (/s) counter for http2priorityframesrcvd
http2rststreamframesrcvd	<Double>	Read-only	Number of HTTP/2 RST_STREAM frames received
http2rststreamframesrcvdrate	<Double>	Read-only	Rate (/s) counter for http2rststreamframesrcvd
http2settingframesrcvd	<Double>	Read-only	Number of HTTP/2 SETTINGS frames received
http2settingframesrcvdrate	<Double>	Read-only	Rate (/s) counter for http2settingframesrcvd
http2pushpromframesrcvd	<Double>	Read-only	Number of HTTP/2 PUSH_PROMISE frames received
http2pushpromframesrcvdrate	<Double>	Read-only	Rate (/s) counter for http2pushpromframesrcvd
http2pingframesrcvd	<Double>	Read-only	Number of HTTP/2 PING frames received
http2pingframesrcvdrate	<Double>	Read-only	Rate (/s) counter for http2pingframesrcvd

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
http2goawayframesrcvd	<Double>	Read-only	Number of HTTP/2 GOAWAY frames received
http2goawayframesrcvdrate	<Double>	Read-only	Rate (/s) counter for http2goawayframesrcvd
http2winupdateframesrcvd	<Double>	Read-only	Number of HTTP/2 WINDOW_UPDATE frames received
http2winupdateframesrcvdrate	<Double>	Read-only	Rate (/s) counter for http2winupdateframesrcvd
http2continuationframesrcvd	<Double>	Read-only	Number of HTTP/2 CONTINUATION frames received
http2continuationframesrcvdrate	<Double>	Read-only	Rate (/s) counter for http2continuationframesrcvd
http2indataframes	<Double>	Read-only	Number of HTTP/2 DATA frames
http2indataframesrate	<Double>	Read-only	Rate (/s) counter for http2indataframes
http2inheaderframes	<Double>	Read-only	Number of HTTP/2 HEADER frames
http2inheaderframesrate	<Double>	Read-only	Rate (/s) counter for http2inheaderframes
http2inpriorityframes	<Double>	Read-only	Number of HTTP/2 PRIORITY frames
http2inpriorityframesrate	<Double>	Read-only	Rate (/s) counter for http2inpriorityframes

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
http2inrststreamframes	<Double>	Read-only	Number of HTTP/2 RST_STREAM frames
http2inrststreamframesrate	<Double>	Read-only	Rate (/s) counter for http2inrststreamframes
http2insettingframes	<Double>	Read-only	Number of HTTP/2 SETTINGS frames
http2insettingframesrate	<Double>	Read-only	Rate (/s) counter for http2insettingframes
http2inpushpromiseframes	<Double>	Read-only	Number of HTTP/2 PUSH_PROMISE frames
http2inpushpromiseframesrate	<Double>	Read-only	Rate (/s) counter for http2inpushpromiseframes
http2inpingframes	<Double>	Read-only	Number of HTTP/2 PING frames
http2inpingframesrate	<Double>	Read-only	Rate (/s) counter for http2inpingframes
http2ingoawayframes	<Double>	Read-only	Number of HTTP/2 GOAWAY frames
http2ingoawayframesrate	<Double>	Read-only	Rate (/s) counter for http2ingoawayframes
http2inwindowupdateframes	<Double>	Read-only	Number of HTTP/2 WINDOW_UPDATE frames

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
http2inwindowupdate framesrate	<Double>	Read-only	Rate (/s) counter for http2inwindowupdate frames
http2incontinuationfr ames	<Double>	Read-only	Number of HTTP/2 CONTINUATION frames
http2incontinuationfr amesrate	<Double>	Read-only	Rate (/s) counter for http2incontinuationfr ames
http2frametoobig	<Double>	Read-only	Number of HTTP/2 frames received carrying a frame length greater than SETTINGS_MAX_F RAME_SIZE sent by NetScale
http2frametoobigrate	<Double>	Read-only	Rate (/s) counter for http2frametoobig
http2pingflood	<Double>	Read-only	HTTP/2 number of ping frames received on connection is above rate limit
http2pingfloodrate	<Double>	Read-only	Rate (/s) counter for http2pingflood
http2errsetflood	<Double>	Read-only	HTTP/2 number of settings frames received on connection is above rate limit
http2errsetfloodrate	<Double>	Read-only	Rate (/s) counter for http2errsetflood

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
http2errresfraflood	<Double>	Read-only	HTTP/2 number of reset frames sent on connection is above rate limit
http2errresfrafloodrate	<Double>	Read-only	Rate (/s) counter for http2errresfraflood
http2errempfraflood	<Double>	Read-only	HTTP/2 number of empty frames received on connection is above rate limit
http2errempfrafloodrate	<Double>	Read-only	Rate (/s) counter for http2errempfraflood
http2errrxresfraflood	<Double>	Read-only	HTTP/2 number of reset frames received on connection is above rate limit
http2errrxresfrafloodrate	<Double>	Read-only	Rate (/s) counter for http2errrxresfraflood

Operations

(click to see Properties)

- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/protocolhttp2 **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/protocolhttp2? **args=detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get protocolhttp2 resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/protocolhttp2? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "protocolhttp2": [ {

"http2inpushpromiseframesrate":<Double_value>,

"http2errempfraflood":<Double_value>,

"http2serverupgradefailed":<Double_value>,

"http2rststreamframesrcvd":<Double_value>,

"http2pingframessentrate":<Double_value>,

"http2goawayframesrcvdrate":<Double_value>,

"http2requestsrate":<Double_value>,

"http2rststreamframesrcvdrate":<Double_value>,

"http2grpcfailurerate":<Double_value>,

"http2inheaderframesrate":<Double_value>,

"http2totgrpcrequest":<Double_value>,

"http2pushpromiseframessent":<Double_value>,

"http2settingframessentrate":<Double_value>,

"http2errresfraflood":<Double_value>,

"http2inpriorityframesrate":<Double_value>,

"http2pingfloodrate":<Double_value>,

"http2inpushpromiseframes":<Double_value>,

"http2frametoobig":<Double_value>,

"http2pingframesrcvd":<Double_value>,
```

```
"http2windowupdateframessentrate":<Double_value>,

"http2altsvcframessentrate":<Double_value>,

"http2frametoobigrate":<Double_value>,

"http2responses":<Double_value>,

"http2totgrpcsuccess":<Double_value>,

"http2nomatcipher":<Double_value>,

"http2errsetfloodrate":<Double_value>,

"http2requestupgradefailed":<Double_value>,

"http2pushpromframesrcvd":<Double_value>,

"http2priorityframessentrate":<Double_value>,

"http2nomatcipherrate":<Double_value>,

"http2errsetflood":<Double_value>,

"http2grpcsuccessrate":<Double_value>,

"http2dataframesrcvd":<Double_value>,

"http2requpg":<Double_value>,

"http2headerframessentrate":<Double_value>,

"http2responsesrate":<Double_value>,

"http2incontinuationframesrate":<Double_value>,

"http2priorityframessent":<Double_value>,

"http2winupdateframesrcvd":<Double_value>,

"http2inpriorityframes":<Double_value>,

"http2pushpromiseframessentrate":<Double_value>,
```

```
"http2directrate":<Double_value>,

"http2headerframesrcvdrate":<Double_value>,

"http2headerframessent":<Double_value>,

"http2goawayframesrcvd":<Double_value>,

"http2dataframessentrate":<Double_value>,

"http2ingoawayframesrate":<Double_value>,

"http2incontinuationframes":<Double_value>,

"http2pingflood":<Double_value>,

"http2continuationframessent":<Double_value>,

"http2priorityframesrcvd":<Double_value>,

"http2inrststreamframesrate":<Double_value>,

"http2winupdateframesrcvdrate":<Double_value>,

"http2pushpromframesrcvdrate":<Double_value>,

"http2inpingframes":<Double_value>,

"http2direct":<Double_value>,

"http2priorityframesrcvdrate":<Double_value>,

"http2totgrpcresponse":<Double_value>,

"http2continuationframessentrate":<Double_value>,

"http2dataframesrcvdrate":<Double_value>,

"http2headerframesrcvd":<Double_value>,

"http2goawayframessent":<Double_value>,

"http2totgrpcfailure":<Double_value>,
```

```
"http2indataframesrate":<Double_value>,

"http2ingoawayframes":<Double_value>,

"http2windowupdateframessent":<Double_value>,

"http2requpgrate":<Double_value>,

"http2serverdirect":<Double_value>,

"http2rststreamframessentrate":<Double_value>,

"http2goawayframessentrate":<Double_value>,

"http2grpcresponserate":<Double_value>,

"http2settingframesrcvdrate":<Double_value>,

"http2dataframessent":<Double_value>,

"http2inwindowupdateframesrate":<Double_value>,

"http2rststreamframessent":<Double_value>,

"http2errresfrafloodrate":<Double_value>,

"http2requests":<Double_value>,

"http2serverdirectfailed":<Double_value>,

"http2inheaderframes":<Double_value>,

"http2insettingframes":<Double_value>,

"http2errrxresfraflood":<Double_value>,

"http2serverupgradefailedrate":<Double_value>,

"http2pingframessent":<Double_value>,

"http2inpingframesrate":<Double_value>,

"http2continuationframesrcvd":<Double_value>,
```

```
"http2errempfrafloodrate":<Double_value>,

"http2errrxresfrafloodrate":<Double_value>,

"http2serverdirectfailedrate":<Double_value>,

"http2requestupgradefailedrate":<Double_value>,

"http2serverdirectrate":<Double_value>,

"http2insettingframesrate":<Double_value>,

"http2inwindowupdateframes":<Double_value>,

"http2settingframessent":<Double_value>,

"http2altsvcframessent":<Double_value>,

"http2grpcrequestrate":<Double_value>,

"http2indataframes":<Double_value>,

"http2settingframesrcvd":<Double_value>,

"http2pingframesrcvdrate":<Double_value>,

"http2continuationframesrcvdrate":<Double_value>,

"http2inrststreamframes":<Double_value>

}]}
```

protocolhttp3

Statistics for http3 resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full
http3requestsrcvd	<Double>	Read-only	Total number of HTTP/3 requests received
http3requestsrcvdrate	<Double>	Read-only	Rate (/s) counter for http3requestsrcvd
http3requestssent	<Double>	Read-only	Total number of HTTP/3 requests sent
http3requestssentrate	<Double>	Read-only	Rate (/s) counter for http3requestssent
http3responsesrcvd	<Double>	Read-only	Total number of HTTP/3 responses received
http3responsesrcvdrate	<Double>	Read-only	Rate (/s) counter for http3responsesrcvd
http3responsessent	<Double>	Read-only	Total number of HTTP/3 responses sent
http3responsessentrate	<Double>	Read-only	Rate (/s) counter for http3responsessent
http3conninfalcfail	<Double>	Read-only	Number of HTTP/3 connection-info allocation failures
http3conninfalcfailrate	<Double>	Read-only	Rate (/s) counter for http3conninfalcfail

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
http3nsbalcfail	<Double>	Read-only	Number of HTTP/3 NSB allocation failures
http3nsbalcfailrate	<Double>	Read-only	Rate (/s) counter for http3nsbalcfail
http3strminfalcfail	<Double>	Read-only	Number of HTTP/3 stream-info allocation failures
http3strminfalcfailrate	<Double>	Read-only	Rate (/s) counter for http3strminfalcfail
http3strmpcbalcfail	<Double>	Read-only	Number of HTTP/3 stream PCB allocation failures
http3strmpcbalcfailrate	<Double>	Read-only	Rate (/s) counter for http3strmpcbalcfail

Operations

(click to see Properties)

- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of

creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/protocolhttp3 **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/protocolhttp3? **args=detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get protocolhttp3 resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/protocolhttp3? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "protocolhttp3": [ {

"http3nsbalcfail":<Double_value>,

"http3requestssentrate":<Double_value>,

"http3responsesrcvd":<Double_value>,

"http3responsessent":<Double_value>,

"http3strminfalcfailrate":<Double_value>,

"http3conninfalcfail":<Double_value>,

"http3strmpcbalcfail":<Double_value>,

"http3requestssent":<Double_value>,

"http3conninfalcfailrate":<Double_value>,

"http3strminfalcfail":<Double_value>,

"http3requestsrcvdrate":<Double_value>,

"http3responsesrcvdrate":<Double_value>,

"http3nsbalcfailrate":<Double_value>,

"http3strmpcbalcfailrate":<Double_value>,

"http3responsessentrate":<Double_value>,

"http3requestsrcvd":<Double_value>

}]}
```

protocolicmp

Statistics for icmp resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full
icmptotrxpkts	<Double>	Read-only	ICMP packets received.
icmprxpktsrate	<Double>	Read-only	Rate (/s) counter for icmptotrxpkts
icmptotrxbytes	<Double>	Read-only	Bytes of ICMP data received.
icmprxbytesrate	<Double>	Read-only	Rate (/s) counter for icmptotrxbytes
icmptottxpkts	<Double>	Read-only	ICMP packets transmitted.
icmptxpktsrate	<Double>	Read-only	Rate (/s) counter for icmptottxpkts
icmptottxbytes	<Double>	Read-only	Bytes of ICMP data transmitted.
icmptxbytesrate	<Double>	Read-only	Rate (/s) counter for icmptottxbytes
icmptotrxechoreply	<Double>	Read-only	ICMP Ping echo replies received.
icmprxechoreplyrate	<Double>	Read-only	Rate (/s) counter for icmptotrxechoreply
icmptottxechoreply	<Double>	Read-only	ICMP Ping echo replies transmitted.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
icmptxechoreplyrate	<Double>	Read-only	Rate (/s) counter for icmptottxechoreply
icmptotrxecho	<Double>	Read-only	ICMP Ping Echo Request and Echo Reply packets received.
icmprxechorate	<Double>	Read-only	Rate (/s) counter for icmptotrxecho
icmptotdstiplookup	<Double>	Read-only	Total number of MTU lookup on destination IP info received on a need fragmentation ICMP error message failed.
icmpcurratethreshold	<Double>	Read-only	Limit for ICMP packets handled every 10 milliseconds. Default value, 0, applies no limit. This is a configurable value using the set rateControl command.
icmptotportunreachablerx	<Double>	Read-only	ICMP Port Unreachable error messages received. This error is generated when there is no service is running on the port.
icmptotportunreachabletx	<Double>	Read-only	ICMP Port Unreachable error messages generated. This error

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			is generated when there is no service is running on the port.
icmptotneedfragrx	<Double>	Read-only	ICMP Fragmentation Needed error messages received for packets that need to be fragmented but for which Don't Fragment is specified the header.
icmptotthresholdexceeds	<Double>	Read-only	Times the ICMP rate threshold is exceeded. If this counter continuously increases, first make sure the ICMP packets received are genuine. If they are, increase the current rate threshold.
icmptotpktsdropped	<Double>	Read-only	ICMP packets dropped because the rate threshold has been exceeded.
icmptotbadchecksum	<Double>	Read-only	ICMP Fragmentation Needed error messages received with an ICMP checksum error.
icmptotnonfirstipfrag	<Double>	Read-only	ICMP Fragmentation Needed error messages received that were generated by an IP fragment

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			other than the first one.
icmptotinvalidbodylen	<Double>	Read-only	ICMP Fragmentation Needed error messages received that specified an invalid body length.
icmptotnotcpconn	<Double>	Read-only	ICMP Need Fragmentation error messages received for TCP packets. The state of the connection for these packets is not maintained on the Citrix ADC.
icmptotnoudpconn	<Double>	Read-only	ICMP Need Fragmentation error messages received for UDP packets. The state of the connection for these packets is not maintained on the Citrix ADC.
icmptotinvalidtcpseqno	<Double>	Read-only	ICMP Fragmentation Needed error messages received for packets that contain an invalid TCP address.
icmptotinvalidnextmtuval	<Double>	Read-only	ICMP Fragmentation Needed error messages received in which the Maximum Transmission Unit

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			(MTU) for the next hop is out of range. The range for the MTU is 576-1500.
icmptotbignextmtu	<Double>	Read-only	ICMP Fragmentation Needed error messages received in which the value for the next MTU is higher than that of the current MTU.
icmptotinvalidprotocol	<Double>	Read-only	ICMP Fragmentation Needed error messages received that contain a protocol other than TCP and UDP.
icmptotbadpmtuipchecksum	<Double>	Read-only	ICMP Fragmentation Needed error messages received with an IP checksum error.
icmptotpmtunolink	<Double>	Read-only	ICMP Fragmentation Needed error messages received on a Protocol Control Block (PCB) with no link. The PCB maintains the state of the connection.
icmptotpmtudiscoverydisabled	<Double>	Read-only	ICMP Need Fragmentation error messages received when the PMTU Discovery mode is not enabled.

Operations

(click to see Properties)

- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/protocolicmp **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/protocolicmp? **args=detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get protocolicmp resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/protocolicmp? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "protocolicmp": [ {

"icmptottxbytes":<Double_value>,

"icmprxpktsrate":<Double_value>,

"icmptotpktsdropped":<Double_value>,

"icmptotinvalidbodylen":<Double_value>,

"icmprxechoreplyrate":<Double_value>,

"icmptotpmtudiscoverydisabled":<Double_value>,

"icmptxpktsrate":<Double_value>,

"icmptxechoreplyrate":<Double_value>,

"icmptotrxbytes":<Double_value>,

"icmptotinvalidnextmtuval":<Double_value>,

"icmptotinvalidtcpseqno":<Double_value>,
```

```
"icmptotrxpkts":<Double_value>,

"icmptotneedfragrx":<Double_value>,

"icmprxbytesrate":<Double_value>,

"icmptottxechoreply":<Double_value>,

"icmptotrxecho":<Double_value>,

"icmptotnotcpconn":<Double_value>,

"icmptotbadpmtuipchecksum":<Double_value>,

"icmpcurratethreshold":<Double_value>,

"icmptotthresholdexceeds":<Double_value>,

"icmptotportunreachablerx":<Double_value>,

"icmptotportunreachabletx":<Double_value>,

"icmptotdstiplookup":<Double_value>,

"icmptxbytesrate":<Double_value>,

"icmptotnonfirstipfrag":<Double_value>,

"icmptotnoudpconn":<Double_value>,

"icmptotpmtunolink":<Double_value>,

"icmptotbignextmtu":<Double_value>,

"icmptottxpkts":<Double_value>,

"icmptotinvalidprotocol":<Double_value>,

"icmptotrxechoreply":<Double_value>,

"icmptotbadchecksum":<Double_value>,

"icmprxechorate":<Double_value>
```

```
}]}
```

protocolicmpv6

Statistics for icmpv6 resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full
icmpv6totrxpkts	<Double>	Read-only	ICMPv6 packets received.
icmpv6rxpktsrate	<Double>	Read-only	Rate (/s) counter for icmpv6totrxpkts
icmpv6totrxbytes	<Double>	Read-only	Bytes of ICMPv6 data received.
icmpv6rxbytesrate	<Double>	Read-only	Rate (/s) counter for icmpv6totrxbytes
icmpv6tottxpkts	<Double>	Read-only	ICMPv6 packets transmitted.
icmpv6txpktsrate	<Double>	Read-only	Rate (/s) counter for icmpv6tottxpkts
icmpv6tottxbytes	<Double>	Read-only	Bytes of ICMPv6 data transmitted.
icmpv6txbytesrate	<Double>	Read-only	Rate (/s) counter for icmpv6tottxbytes

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
icmpv6totrxna	<Double>	Read-only	ICMPv6 neighbor advertisement packets received. These packets are received in response to a neighbor solicitation message sent out by this node, or if the link layer address of a neighbor has changed.
icmpv6rxnarate	<Double>	Read-only	Rate (/s) counter for icmpv6totrxna
icmpv6totrxns	<Double>	Read-only	ICMPv6 neighbor solicitation packets received. These packets are received if the link layer address of a neighbor has changed, or in response to a neighbor solicitation message sent out by this node.
icmpv6rxnsrate	<Double>	Read-only	Rate (/s) counter for icmpv6totrxns
icmpv6totrxra	<Double>	Read-only	ICMPv6 router advertisement packets received. These are received at defined intervals or in response to a router solicitation message.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
icmpv6rxrarate	<Double>	Read-only	Rate (/s) counter for icmpv6totrxra
icmpv6totrxrs	<Double>	Read-only	ICMPv6 router solicitation packets received. These could be sent by a neighboring router to initiate address resolution.
icmpv6rxrsrate	<Double>	Read-only	Rate (/s) counter for icmpv6totrxrs
icmpv6totrxechoreq	<Double>	Read-only	ICMPv6 Ping Echo Request packets received.
icmpv6rxechoreqrate	<Double>	Read-only	Rate (/s) counter for icmpv6totrxechoreq
icmpv6totrxechoreply	<Double>	Read-only	ICMPv6 Ping Echo Reply packets received.
icmpv6rxechoreplyrate	<Double>	Read-only	Rate (/s) counter for icmpv6totrxechoreply
icmpv6tottxna	<Double>	Read-only	ICMPv6 neighbor advertisement packets transmitted. These packets are sent in response to a neighbor solicitation packet, or if the link layer address of this node has changed.
icmpv6txnarate	<Double>	Read-only	Rate (/s) counter for icmpv6tottxna

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
icmpv6tottxns	<Double>	Read-only	ICMPv6 neighbor solicitation packets transmitted. These packets are sent to get the link layer addresses of neighboring nodes or to confirm that they are reachable.
icmpv6txnsrate	<Double>	Read-only	Rate (/s) counter for icmpv6tottxns
icmpv6tottxra	<Double>	Read-only	ICMPv6 router advertisement packets transmitted. These packets are sent at regular intervals or in response to a router solicitation packet from a neighbor.
icmpv6txrarate	<Double>	Read-only	Rate (/s) counter for icmpv6tottxra
icmpv6tottxrs	<Double>	Read-only	ICMPv6 router solicitation packets transmitted. These packets are sent to request neighboring routers to generate router advertisements immediately rather than wait for the next defined time.
icmpv6txrsrate	<Double>	Read-only	Rate (/s) counter for icmpv6tottxrs

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
icmpv6tottxechoreq	<Double>	Read-only	ICMPv6 Ping Echo Request packets transmitted.
icmpv6txechoreqrate	<Double>	Read-only	Rate (/s) counter for icmpv6tottxechoreq
icmpv6tottxechoreply	<Double>	Read-only	ICMP Ping Echo Reply packets transmitted.
icmpv6txechoreplyrate	<Double>	Read-only	Rate (/s) counter for icmpv6tottxechoreply
icmpv6errra	<Double>	Read-only	ICMPv6 router advertisement error packets received that contain an error in the header, such as an incorrect source IP address, destination IP address, or packet length.
icmpv6errna	<Double>	Read-only	ICMPv6 neighbor advertisement error packets received that contain an error in the header, such as an incorrect source IP address, destination IP address, or packet length.
icmpv6errns	<Double>	Read-only	ICMPv6 neighbor solicitation error packets received that contain an error in the header, such as

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			an incorrect source IP address, destination IP address, or packet length.
icmpv6badchecksums	<Double>	Read-only	Packets received with an ICMPv6 checksum error.
icmpv6unspt	<Double>	Read-only	ICMPv6 packets received that are not supported by the Citrix ADC.
icmpv6rtthsld	<Double>	Read-only	Packets dropped because the default threshold of 100 requests per 10 milliseconds has been exceeded. This is a configurable value using the set rateControl command.

Operations

(click to see Properties)

- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/protocolicmpv6 **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/protocolicmpv6? **args=detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get protocolicmpv6 resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/protocolicmpv6? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "protocolicmpv6": [ {

"icmpv6rxnsrate":<Double_value>,

"icmpv6txnarate":<Double_value>,

"icmpv6totrxra":<Double_value>,

"icmpv6totrxrs":<Double_value>,

"icmpv6tottxrs":<Double_value>,

"icmpv6tottxra":<Double_value>,

"icmpv6txbytesrate":<Double_value>,

"icmpv6rxechoreqrate":<Double_value>,

"icmpv6rxrarate":<Double_value>,

"icmpv6tottxechoreq":<Double_value>,

"icmpv6totrxechoreply":<Double_value>,

"icmpv6tottxechoreply":<Double_value>,

"icmpv6totrxechoreq":<Double_value>,

"icmpv6rxechoreplyrate":<Double_value>,

"icmpv6txpktsrate":<Double_value>,

"icmpv6txrsrate":<Double_value>,

"icmpv6rxpktsrate":<Double_value>,

"icmpv6rxrsrate":<Double_value>,

"icmpv6totrxna":<Double_value>,
```

```
"icmpv6totrxns":<Double_value>,

"icmpv6tottxns":<Double_value>,

"icmpv6tottxna":<Double_value>,

"icmpv6txechoreplyrate":<Double_value>,

"icmpv6unspt":<Double_value>,

"icmpv6txrarate":<Double_value>,

"icmpv6rtthsld":<Double_value>,

"icmpv6rxbytesrate":<Double_value>,

"icmpv6txechoreqrate":<Double_value>,

"icmpv6errra":<Double_value>,

"icmpv6tottxpkts":<Double_value>,

"icmpv6rxnarate":<Double_value>,

"icmpv6totrxpkts":<Double_value>,

"icmpv6tottxbytes":<Double_value>,

"icmpv6totrxbytes":<Double_value>,

"icmpv6badchecksums":<Double_value>,

"icmpv6errns":<Double_value>,

"icmpv6txnsrate":<Double_value>,

"icmpv6errna":<Double_value>

}]}
```

protocolip

Statistics for protocolip resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full
iptotrxpkts	<Double>	Read-only	IP packets received.
iprxpktsrate	<Double>	Read-only	Rate (/s) counter for iptotrxpkts
iptotrxbytes	<Double>	Read-only	Bytes of IP data received.
iprxbytesrate	<Double>	Read-only	Rate (/s) counter for iptotrxbytes
iptottxpkts	<Double>	Read-only	IP packets transmitted.
iptxpktsrate	<Double>	Read-only	Rate (/s) counter for iptottxpkts
iptottxbytes	<Double>	Read-only	Bytes of IP data transmitted.
iptxbytesrate	<Double>	Read-only	Rate (/s) counter for iptottxbytes
iptotrxmbits	<Double>	Read-only	Megabits of IP data received.
iprxmbitsrate	<Double>	Read-only	Rate (/s) counter for iptotrxmbits

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
iptottxmbits	<Double>	Read-only	Megabits of IP data transmitted.
iptxmbitsrate	<Double>	Read-only	Rate (/s) counter for iptottxmbits
iptotroutedpkts	<Double>	Read-only	Total routed packets.
iproutedpktsrate	<Double>	Read-only	Rate (/s) counter for iptotroutedpkts
iptotroutedmbits	<Double>	Read-only	Total routed Mbits
iproutedmbitsrate	<Double>	Read-only	Rate (/s) counter for iptotroutedmbits
iptotroutedbytes	<Double>	Read-only	Total routed IP bytes.
iproutedbytesrate	<Double>	Read-only	Rate (/s) counter for iptotroutedbytes
iptotfragments	<Double>	Read-only	IP fragments received.
iptotsuccreassembly	<Double>	Read-only	Fragmented IP packets successfully reassembled on the Citrix ADC.
iptotreassemblyattempt	<Double>	Read-only	IP packets that the Citrix ADC attempts to reassemble. If one of the fragments is missing, the whole packet is dropped.
iptotaddrlookup	<Double>	Read-only	IP address lookups performed by the Citrix ADC. When a packet is received on a non-established session, the Citrix

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			ADC checks if the destination IP address is one of the Citrix ADC owned IP addresses.
iptotaddrlookupfail	<Double>	Read-only	IP address lookups performed by the Citrix ADC that have failed because the destination IP address of the packet does not match any of the Citrix ADC owned IP addresses.
iptotudpfragmentsfwd	<Double>	Read-only	UDP fragments forwarded to the client or the server.
iptottcpfragmentsfwd	<Double>	Read-only	TCP fragments forwarded to the client or the server.
iptotfragpktsgen	<Double>	Read-only	Fragmented packets created by the Citrix ADC.
iptotbadchecksums	<Double>	Read-only	Packets received with an IP checksum error.
iptotunsuccreassembly	<Double>	Read-only	Packets received that could not be reassembled. This can occur when there is a checksum failure, an identification field mismatch, or when

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			one of the fragments is missing.
iptottoobig	<Double>	Read-only	Packets received for which the reassembled data exceeds the Ethernet packet data length of 1500 bytes.
iptotzerofragmentlen	<Double>	Read-only	Packets received with a fragment length of 0 bytes.
iptotdupfragments	<Double>	Read-only	Duplicate IP fragments received. This can occur when the acknowledgement was not received within the expected time.
iptotoutoforderfrag	<Double>	Read-only	Fragments received that are out of order.
iptotunknowndstrcvd	<Double>	Read-only	Packets received in which the destination IP address was not reachable or not owned by the Citrix ADC.
iptotbadtransport	<Double>	Read-only	Packets received in which the protocol specified in the IP header is unknown to the Citrix ADC.
iptotvipdown	<Double>	Read-only	Packets received for which the VIP is down. This can occur

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			when all the services bound to the VIP are down or the VIP is manually disabled.
iptotfixheaderfail	<Double>	Read-only	Packets received that contain an error in one or more components of the IP header.
iptotttlexpired	<Double>	Read-only	Packets for which the time-to-live (TTL) expired during transit. These packets are dropped.
iptotmaxclients	<Double>	Read-only	Attempts to open a new connection to a service for which the maximum limit has been exceeded. Default value, 0, applies no limit.
iptotunknownsvcs	<Double>	Read-only	Packets received on a port or service that is not configured.
iptotlandattacks	<Double>	Read-only	Land-attack packets received. The source and destination addresses are the same.
iptotinvalidheadersz	<Double>	Read-only	Packets received in which an invalid data length is specified, or the value in the length field and the actual data length do not match. The

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			range for the Ethernet packet data length is 0-1500 bytes.
iptotinvalidpacketsize	<Double>	Read-only	Total number of packets received by Citrix ADC with invalid IP packet size.
iptottruncatedpackets	<Double>	Read-only	Truncated IP packets received. An overflow in the routers along the path can truncate IP packets.
noniptottruncatedpackets	<Double>	Read-only	Truncated non-IP packets received.
iptotzeronexthop	<Double>	Read-only	Packets received that contain a 0 value in the next hop field. These packets are dropped.
iptotbadlens	<Double>	Read-only	Packets received with a length greater than the normal maximum transmission unit of 1514 bytes.
iptotbadmacaddrs	<Double>	Read-only	IP packets transmitted with a bad MAC address.

Operations

(click to see Properties)

- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/protocolip **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/protocolip? **args=detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get protocolip resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/protocolip? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "protocolip": [ {

"iptotlandattacks":<Double_value>,

"iptotrxbytes":<Double_value>,

"iprxbytesrate":<Double_value>,

"iproutedbytesrate":<Double_value>,

"iproutedmbitsrate":<Double_value>,

"iptotbadchecksums":<Double_value>,

"iptotunsuccreassembly":<Double_value>,

"iptottxpkts":<Double_value>,

"iproutedpktsrate":<Double_value>,

"iptotsuccreassembly":<Double_value>,

"iptotoutoforderfrag":<Double_value>,

"iptotbadmacaddrs":<Double_value>,

"iptotbadtransport":<Double_value>,
```

```
"iptottruncatedpackets":<Double_value>,

"iptotroutedmbits":<Double_value>,

"iprxmbitsrate":<Double_value>,

"iptotunknownsvcs":<Double_value>,

"iptotaddrlookup":<Double_value>,

"iptotfragpktsgen":<Double_value>,

"iptottcpfragmentsfwd":<Double_value>,

"iptotinvalidheadersz":<Double_value>,

"iptxpktsrate":<Double_value>,

"iptotrxmbits":<Double_value>,

"iptotfixheaderfail":<Double_value>,

"iprxpktsrate":<Double_value>,

"noniptottruncatedpackets":<Double_value>,

"iptotunknowndstrcvd":<Double_value>,

"iptotzeronexthop":<Double_value>,

"iptottxmbits":<Double_value>,

"iptxmbitsrate":<Double_value>,

"iptottoobig":<Double_value>,

"iptotaddrlookupfail":<Double_value>,

"iptotzerofragmentlen":<Double_value>,

"iptotmaxclients":<Double_value>,

"iptotroutedbytes":<Double_value>,
```

```
"iptotdupfragments":<Double_value>,

"iptotreassemblyattempt":<Double_value>,

"iptotrxpkts":<Double_value>,

"iptotroutedpkts":<Double_value>,

"iptotttlexpired":<Double_value>,

"iptotbadlens":<Double_value>,

"iptotudpfragmentsfwd":<Double_value>,

"iptotinvalidpacketsize":<Double_value>,

"iptotfragments":<Double_value>,

"iptottxbytes":<Double_value>,

"iptotvipdown":<Double_value>,

"iptxbytesrate":<Double_value>

}]}
```

protocolipv6

Statistics for ip v6 resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ipv6totrxpkts	<Double>	Read-only	IPv6 packets received.
ipv6rxpktsrate	<Double>	Read-only	Rate (/s) counter for ipv6totrxpkts
ipv6totrxbytes	<Double>	Read-only	Bytes of IPv6 data received.
ipv6rxbytesrate	<Double>	Read-only	Rate (/s) counter for ipv6totrxbytes
ipv6tottxpkts	<Double>	Read-only	IPv6 packets transmitted
ipv6txpktsrate	<Double>	Read-only	Rate (/s) counter for ipv6tottxpkts
ipv6tottxbytes	<Double>	Read-only	Bytes of IPv6 data transmitted.
ipv6txbytesrate	<Double>	Read-only	Rate (/s) counter for ipv6tottxbytes
ipv6totroutepkts	<Double>	Read-only	IPv6 packets routed.
ipv6routepktsrate	<Double>	Read-only	Rate (/s) counter for ipv6totroutepkts
ipv6totroutembits	<Double>	Read-only	IPv6 total Mbits.
ipv6routembitsrate	<Double>	Read-only	Rate (/s) counter for ipv6totroutembits
ipv6fragtotrxpkts	<Double>	Read-only	IPv6 fragments received.
ipv6fragrxpktsrate	<Double>	Read-only	Rate (/s) counter for ipv6fragtotrxpkts

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ipv6fragtottcpreassembled	<Double>	Read-only	TCP fragments processed after reassembly.
ipv6fragtcpreassembledrate	<Double>	Read-only	Rate (/s) counter for ipv6fragtottcpreassembled
ipv6fragtotudpreassembled	<Double>	Read-only	UDP fragments processed after reassembly.
ipv6fragudpreassembledrate	<Double>	Read-only	Rate (/s) counter for ipv6fragtotudpreassembled
ipv6fragtotpktsprocessnoreass	<Double>	Read-only	IPv6 fragments processed without reassembly.
ipv6fragpktsprocessnoreassrate	<Double>	Read-only	Rate (/s) counter for ipv6fragtotpktsprocessnoreass
ipv6fragtotpktsforward	<Double>	Read-only	IPv6 fragments forwarded to the client or server without reassembly.
ipv6fragpktsforwardrate	<Double>	Read-only	Rate (/s) counter for ipv6fragtotpktsforward
ipv6errhdr	<Double>	Read-only	Packets received that contain an error in one or more components of the IPv6 header.
ipv6nextheadererr	<Double>	Read-only	Packets received that contain an unsupported next

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			header. The supported next headers are TCP, ICMP, UDP, OSPF, and FRAGMENT.
ipv6landattack	<Double>	Read-only	Land-attack packets received. The source and destination addresses are the same. If not dropped, these packets can lock up the appliance.
ipv6fragpkttoobig	<Double>	Read-only	Packets received for which the reassembled data exceeds the Ethernet packet data length of 1500 bytes.
ipv6fragzerolenpkt	<Double>	Read-only	Packets received with a fragment length of 0 bytes.
ipv6toticmpnarx	<Double>	Read-only	Number of ICMPv6 NA packets received by Citrix ADC (OBSOLETE).
ipv6icmpnarxrate	<Double>	Read-only	Rate (/s) counter for ipv6toticmpnarx
ipv6toticmpnsrx	<Double>	Read-only	Number of ICMPv6 NS packets received by Citrix ADC (OBSOLETE).
ipv6icmpnsrxrate	<Double>	Read-only	Rate (/s) counter for ipv6toticmpnsrx

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ipv6toticmpnatx	<Double>	Read-only	Number of ICMPv6 NA packets transmitted by Citrix ADC (OBSOLETE).
ipv6icmpnatxrate	<Double>	Read-only	Rate (/s) counter for ipv6toticmpnatx
ipv6toticmpnstx	<Double>	Read-only	Number of ICMPv6 NS packets transmitted by Citrix ADC (OBSOLETE).
ipv6icmpnstxrate	<Double>	Read-only	Rate (/s) counter for ipv6toticmpnstx
ipv6toticmprarx	<Double>	Read-only	Number of ICMPv6 RA packets received by Citrix ADC (OBSOLETE).
ipv6icmprarxrate	<Double>	Read-only	Rate (/s) counter for ipv6toticmprarx
ipv6toticmprstx	<Double>	Read-only	Number of ICMPv6 RS packets transmitted by Citrix ADC (OBSOLETE).
ipv6icmprstxrate	<Double>	Read-only	Rate (/s) counter for ipv6toticmprstx
ipv6toticmprx	<Double>	Read-only	Number of ICMPv6 packets received by Citrix ADC (OBSOLETE).
ipv6icmprxrate	<Double>	Read-only	Rate (/s) counter for ipv6toticmprx

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ipv6toticmptx	<Double>	Read-only	Number of ICMPv6 packets transmitted by Citrix ADC (OBSOLETE).
ipv6icmptxrate	<Double>	Read-only	Rate (/s) counter for ipv6toticmptx
ipv6errrxhdr	<Double>	Read-only	Number of erroneous header packets received (OBSOLETE).
ipv6errrxpkt	<Double>	Read-only	Number of erroneous packets received (OBSOLETE).
ipv6badcksum	<Double>	Read-only	Number of bad checksum packets received (OBSOLETE).
icmpv6error	<Double>	Read-only	Number of erroneous ICMPv6 packets received (OBSOLETE).
icmpv6unspt	<Double>	Read-only	Number of ICMPv6 unsupported packets received (OBSOLETE).
icmpv6rtthsld	<Double>	Read-only	Number of ICMPv6 packets dropped for rate threshold exceeded (OBSOLETE).

Operations

(click to see Properties)

- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/protocolipv6 **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/protocolipv6? **args=detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get protocolipv6 resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/protocolipv6? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "protocolipv6": [ {

"ipv6fragtottcpreassembled":<Double_value>,

"ipv6rxbytesrate":<Double_value>,

"ipv6totrxpkts":<Double_value>,

"ipv6landattack":<Double_value>,

"ipv6icmprarxrate":<Double_value>,

"icmpv6error":<Double_value>,

"ipv6totroutepkts":<Double_value>,

"ipv6errrxpkt":<Double_value>,

"ipv6txbytesrate":<Double_value>,

"ipv6fragrxpktsrate":<Double_value>,

"ipv6toticmprx":<Double_value>,

"ipv6icmpnstxrate":<Double_value>,

"ipv6routepktsrate":<Double_value>,
```

```
"ipv6nextheadererr":<Double_value>,

"ipv6toticmpnarx":<Double_value>,

"ipv6toticmpnsrx":<Double_value>,

"ipv6fragtotudpreassembled":<Double_value>,

"ipv6tottxpkts":<Double_value>,

"ipv6icmpnsrxrate":<Double_value>,

"ipv6badcksum":<Double_value>,

"ipv6fragudpreassembledrate":<Double_value>,

"icmpv6rtthsld":<Double_value>,

"ipv6toticmprstx":<Double_value>,

"icmpv6unspt":<Double_value>,

"ipv6fragtotrxpkts":<Double_value>,

"ipv6rxpktsrate":<Double_value>,

"ipv6icmpnarxrate":<Double_value>,

"ipv6toticmprarx":<Double_value>,

"ipv6tottxbytes":<Double_value>,

"ipv6icmprxrate":<Double_value>,

"ipv6fragpkttoobig":<Double_value>,

"ipv6errhdr":<Double_value>,

"ipv6icmprstxrate":<Double_value>,

"ipv6errrxhdr":<Double_value>,

"ipv6txpktsrate":<Double_value>,
```

```
"ipv6icmptxrate":<Double_value>,

"ipv6toticmpnatx":<Double_value>,

"ipv6toticmpnstx":<Double_value>,

"ipv6toticmptx":<Double_value>,

"ipv6fragzerolenpkt":<Double_value>,

"ipv6fragpktsforwardrate":<Double_value>,

"ipv6fragtotpktsforward":<Double_value>,

"ipv6totrxbytes":<Double_value>,

"ipv6totroutembits":<Double_value>,

"ipv6routembitsrate":<Double_value>,

"ipv6fragtotpktsprocessnoreass":<Double_value>,

"ipv6fragpktsprocessnoreassrate":<Double_value>,

"ipv6icmpnatxrate":<Double_value>,

"ipv6fragtcpreassembledrate":<Double_value>

}]}
```

protocolmptcp

Statistics for mptcp protocol resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
clearstats	<String>	Read-write	Clear the statsistics / counters.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = basic, full
mptcptotmpcapsession	<Double>	Read-only	MPTCP total sessions created
mptcpmpcapsessionrate	<Double>	Read-only	Rate (/s) counter for mptcptotmpcapsession
mptcptotv1mpcapsession	<Double>	Read-only	MPTCP total V1 sessions created
mptcpv1mpcapsessionrate	<Double>	Read-only	Rate (/s) counter for mptcptotv1mpcapsession
mptcptotsfconn	<Double>	Read-only	MPTCP total Subflow connections created
mptcpsfconnrate	<Double>	Read-only	Rate (/s) counter for mptcptotsfconn
mptcpcurmpcapablesessions	<Double>	Read-only	The number of current mptcp sessions.
mptcpcurv1mpcapablesessions	<Double>	Read-only	The number of current V1 mptcp sessions.
mptcpcursfconnections	<Double>	Read-only	The number of current mptcp subflow connections.
mptcpcurpendingjoin	<Double>	Read-only	The number of current mptcp subflow connections in pending state.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
mptcpcursesswithoutsfs	<Double>	Read-only	Current Multipath TCP sessions without any subflows
mptcptotmpcapsyn	<Double>	Read-only	MPTCP total MP_CAPABLE received
mptcpmpcapsynrate	<Double>	Read-only	Rate (/s) counter for mptcptotmpcapsyn
mptcptotv1mpcapsyn	<Double>	Read-only	MPTCP total Version1 MP_CAPABLE received
mptcpv1mpcapsynrate	<Double>	Read-only	Rate (/s) counter for mptcptotv1mpcapsyn
mptcptotmpcapsteered	<Double>	Read-only	Total MP_CAPABLE sessions steered
mptcpmpcapsteeredrate	<Double>	Read-only	Rate (/s) counter for mptcptotmpcapsteered
mptcptotconnest	<Double>	Read-only	Total MP_CAPABLE sessions created.
mptcpconnestrate	<Double>	Read-only	Rate (/s) counter for mptcptotconnest
mptcptotmpcapsynacksent	<Double>	Read-only	Total number of MP_CAPABLE SYN/ACKs sent.
mptcpmpcapsynacksentrate	<Double>	Read-only	Rate (/s) counter for mptcptotmpcapsynacksent

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
mptcptotmpcapfackrecvd	<Double>	Read-only	Total number of MP_CAPABLE Final ACKs received.
mptcpmpcapfackrecvdrate	<Double>	Read-only	Rate (/s) counter for mptcptotmpcapfackrecvd
mptcptotmpjoinsyn	<Double>	Read-only	MPTCP total MP_JOIN syn received
mptcpmpjoinsynrate	<Double>	Read-only	Rate (/s) counter for mptcptotmpjoinsyn
mptcptotmpjoinsteered	<Double>	Read-only	Total MP_JOIN subflows steered
mptcpmpjoinsteeredrate	<Double>	Read-only	Rate (/s) counter for mptcptotmpjoinsteered
mptcptotmpjoinsynacksent	<Double>	Read-only	Total MP_JOIN SYN/ACKs sent.
mptcpmpjoinsynacksentrate	<Double>	Read-only	Rate (/s) counter for mptcptotmpjoinsynacksent
mptcptotmpjoinfackrecvd	<Double>	Read-only	Total number of MP_JOIN Final ACKs
mptcpmpjoinfackrecvdrate	<Double>	Read-only	Rate (/s) counter for mptcptotmpjoinfackrecvd
mptcptotmpjoin4thacksent	<Double>	Read-only	Total number of Subflow final ACK from peer in 3 way

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			handshake validated with 4th ACK.
mptcpmpjoin4thacksentrate	<Double>	Read-only	Rate (/s) counter for mptcptotmpjoin4thacksent
mptcptotestsfreplaced	<Double>	Read-only	MPTCP Total established subflows replaced due to new MP_JOIN.
mptcpestsfreplacedrate	<Double>	Read-only	Rate (/s) counter for mptcptotestsfreplaced
mptcptotpendsfreplaced	<Double>	Read-only	MPTCP Total pending subflows replaced due to new MP_JOIN.
mptcppendsfreplacedrate	<Double>	Read-only	Rate (/s) counter for mptcptotpendsfreplaced
mptcptotfreshackfrwd	<Double>	Read-only	Fresh ACK recieved on a subflow
mptcpfreshackfrwdrate	<Double>	Read-only	Rate (/s) counter for mptcptotfreshackfrwd
mptcpplainackfallback	<Double>	Read-only	MPTCP Fallback to regular tcp on receiving plain ACK for DSS.
mptcpplainackfallbackrate	<Double>	Read-only	Rate (/s) counter for mptcpplainackfallback

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
mptcpinfinitemaprecvd	<Double>	Read-only	MPTCP Received and set infinite map and fallen back to regular TCP.
mptcpinfinitemaprecvdrate	<Double>	Read-only	Rate (/s) counter for mptcpinfinitemaprecvd
mptcptotaddrremoved	<Double>	Read-only	Total number of addresses removed from MPTCP connection with REMOVE_ADDR option
mptcpaddrremovedrate	<Double>	Read-only	Rate (/s) counter for mptcptotaddrremoved
mptcptotdss	<Double>	Read-only	Total number of Data Sequence Signal packets.
mptcpdssrate	<Double>	Read-only	Rate (/s) counter for mptcptotdss
mptcptotrxdss	<Double>	Read-only	MPTCP Total Data Sequence Signal packets received.
mptcprxdssrate	<Double>	Read-only	Rate (/s) counter for mptcptotrxdss
mptcptottxdss	<Double>	Read-only	MMPTCP Total Data Sequence Signal packets sent
mptcptxdssrate	<Double>	Read-only	Rate (/s) counter for mptcptottxdss

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
mptcptotdssa	<Double>	Read-only	Total Data Sequence Signal packets during data transfer with DATA_ACK
mptcpdssarate	<Double>	Read-only	Rate (/s) counter for mptcptotdssa
mptcptotdssfreshack	<Double>	Read-only	MPTCP total Data Sequence Signal packets during data transfer with fresh ACK
mptcpdssfreshackrate	<Double>	Read-only	Rate (/s) counter for mptcptotdssfreshack
mptcptotdssm	<Double>	Read-only	MPTCP total data Sequence Signal packets with Data Sequence Mapping and checksum
mptcpdssmrate	<Double>	Read-only	Rate (/s) counter for mptcptotdssm
mptcptotinfinitemapfrwd	<Double>	Read-only	MPTCP received Data Sequence Signal with infinite map flag (Fallback to regular TCP).
mptcpinfinitemapfrwdrate	<Double>	Read-only	Rate (/s) counter for mptcptotinfinitemapfrwd
mptcptotdatalessthandatalen	<Double>	Read-only	MPTCP Map amount of data not yet received.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
mptcpdatalessthandatalenrate	<Double>	Read-only	Rate (/s) counter for mptcptotdatalessthandatalen
mptcppriobackuprx	<Double>	Read-only	MPTCP Subflow used as backup path.
mptcppriobackuprxrate	<Double>	Read-only	Rate (/s) counter for mptcppriobackuprx
mptcpprioclearbackuprx	<Double>	Read-only	Subflow earlier used only as a backup subflow, changes to regular subflow with MP_PRIO option
mptcpprioclearbackuprxrate	<Double>	Read-only	Rate (/s) counter for mptcpprioclearbackuprx
mptcptottxdatafin	<Double>	Read-only	Total MPTCP connection close requests sent
mptcptxdatafinrate	<Double>	Read-only	Rate (/s) counter for mptcptottxdatafin
mptcptotrxdatafin	<Double>	Read-only	Total MPTCP connection close(DATA_FIN) requests received.
mptcprxdatafinrate	<Double>	Read-only	Rate (/s) counter for mptcptotrxdatafin
mptcptottxsffin	<Double>	Read-only	MPTCP total subflow close requests.
mptcptxsffinrate	<Double>	Read-only	Rate (/s) counter for mptcptottxsffin

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
mptcperrinvalcookie	<Double>	Read-only	MPTCP invalid cookie received on MP_CAPABLE final ACK.
mptcperrinvalcookierate	<Double>	Read-only	Rate (/s) counter for mptcperrinvalcookie
mptcperrextnflagset	<Double>	Read-only	Extension flag is set on MP_CAPABLE request.
mptcperrextnflagsetrate	<Double>	Read-only	Rate (/s) counter for mptcperrextnflagset
mptcperrresflagset	<Double>	Read-only	MPTCP One or more reserved bits are set on MP_CAPABLE request.
mptcperrresflagsetrate	<Double>	Read-only	Rate (/s) counter for mptcperrresflagset
mptcperrunknowntoken	<Double>	Read-only	MPTCP invalid token received on MP_JOIN request.
mptcperrunknowntokenrate	<Double>	Read-only	Rate (/s) counter for mptcperrunknowntoken
mptcperraddridexist	<Double>	Read-only	MPTCP MP_JOIN request on existing address id.
mptcperraddridexistrate	<Double>	Read-only	Rate (/s) counter for mptcperraddridexist
mptcperraddrid0	<Double>	Read-only	MPTCP MP_JOIN request on address id 0.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
mptcperraddrid0rate	<Double>	Read-only	Rate (/s) counter for mptcperraddrid0
mptcperrmaxsf	<Double>	Read-only	MPTCP new MP_JOIN request after maximum configured subflows are established.
mptcperrmaxsfrate	<Double>	Read-only	Rate (/s) counter for mptcperrmaxsf
mptcperrjointhreshold	<Double>	Read-only	MPTCP Global pending MP_JOIN threshold limit is reached, new MP_JOIN request will be dropped sending RST
mptcperrjointhresholdrate	<Double>	Read-only	Rate (/s) counter for mptcperrjointhreshold
mptcperrjoinafterfallback	<Double>	Read-only	MPTCP New MP_JOIN request received after fallback to regular tcp.
mptcperrjoinafterfallbackrate	<Double>	Read-only	Rate (/s) counter for mptcperrjoinafterfallback
mptcperrinvalmac	<Double>	Read-only	MPTCP invalid MAC on MP_JOIN final ACK.
mptcperrinvalmacrate	<Double>	Read-only	Rate (/s) counter for mptcperrinvalmac

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
mptcperrinvalopts	<Double>	Read-only	MPTCP invalid mptcp option is received and is dropped.
mptcperrinvaloptsrate	<Double>	Read-only	Rate (/s) counter for mptcperrinvalopts
mptcperroptiondiscarded	<Double>	Read-only	Invalid subtype in MPTCP option field and hence discarded.
mptcperroptiondiscardedrate	<Double>	Read-only	Rate (/s) counter for mptcperroptiondiscarded
mptcperroptsnosession	<Double>	Read-only	MPTCP options sent on non existing connection/subflow PCBs.
mptcperroptsnosessionrate	<Double>	Read-only	Rate (/s) counter for mptcperroptsnosession
mptcperrinvalremaddr	<Double>	Read-only	MPTCP remove address request received on invalid/ unknown address id.
mptcperrinvalremaddrrate	<Double>	Read-only	Rate (/s) counter for mptcperrinvalremaddr
mptcperroptssendrst	<Double>	Read-only	MPTCP sent RST on receiving improper option field.
mptcperroptssendrstrate	<Double>	Read-only	Rate (/s) counter for mptcperroptssendrst

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
mptcperrremaddrself	<Double>	Read-only	MPTCP remove address request for self address.
mptcperrremaddrself rate	<Double>	Read-only	Rate (/s) counter for mptcperrremaddrself
mptcperrrssffail	<Double>	Read-only	Add RSS filter to steer traffic to right node on established MPTCP session failed.
mptcperrrssffailrate	<Double>	Read-only	Rate (/s) counter for mptcperrrssffail
mptcperrnopayloadle npkt	<Double>	Read-only	MPTCP Payload length not specified in packet.
mptcperrnopayloadle npktrate	<Double>	Read-only	Rate (/s) counter for mptcperrnopayloadle npkt
mptcperrunsupporte dmssnegotiated	<Double>	Read-only	MPTCP Unsupported MSS negotiated error.
mptcperrunsupporte dmssnegotiatedrate	<Double>	Read-only	Rate (/s) counter for mptcperrunsupporte dmssnegotiated
mptcperrbadcksum	<Double>	Read-only	MPTCP checksum failed. Connection will fallback to regular tcp.
mptcperrbadcksumra te	<Double>	Read-only	Rate (/s) counter for mptcperrbadcksum

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
mptcperrcryptonotsupported	<Double>	Read-only	MPTCP client crypto algorithm not supported.
mptcperrcryptonotsupportedrate	<Double>	Read-only	Rate (/s) counter for mptcperrcryptonotsupported
mptcperrversionnotsupported	<Double>	Read-only	MPTCP MP_CAPABLE request from unsupported mptcp client.
mptcperrversionnotsupportedrate	<Double>	Read-only	Rate (/s) counter for mptcperrversionnotsupported
mptcpplainackrst	<Double>	Read-only	MPTCP Sent RST on receiving plain ACK for DSS.
mptcpplainackrstrate	<Double>	Read-only	Rate (/s) counter for mptcpplainackrst
mptcperrdatafinpassive	<Double>	Read-only	MPTCP Data FIN received on passive subflow
mptcperrdatafinpassiverate	<Double>	Read-only	Rate (/s) counter for mptcperrdatafinpassive
mptcperrfastclose	<Double>	Read-only	MPTCP FAST CLOSE sent.
mptcperrfastcloserate	<Double>	Read-only	Rate (/s) counter for mptcperrfastclose

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
mptcperrfastclosepassive	<Double>	Read-only	MPTCP Fast close received on passive subflow.
mptcperrfastclosepassiverate	<Double>	Read-only	Rate (/s) counter for mptcperrfastclosepassive
mptcperrfastclosekey	<Double>	Read-only	MPTCP FAST_CLOSE received with invalid key and the packet is dropped.
mptcperrfastclosekeyrate	<Double>	Read-only	Rate (/s) counter for mptcperrfastclosekey
mptcpmpfailsent	<Double>	Read-only	MPTCP Total MP_FAIL sent due to checksum failure.
mptcpmpfailsentrate	<Double>	Read-only	Rate (/s) counter for mptcpmpfailsent
mptcpmpfailrecvd	<Double>	Read-only	MPTCP Total MP_FAIL received and fallback to regular TCP.
mptcpmpfailrecvdrate	<Double>	Read-only	Rate (/s) counter for mptcpmpfailrecvd
mptcperrnomappktrcvd	<Double>	Read-only	MPTCP Packet received with no Data Sequence Mapping.
mptcperrnomappktrcvdrate	<Double>	Read-only	Rate (/s) counter for mptcperrnomappktrcvd

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
mptcptotmoredatarcvd	<Double>	Read-only	MPTCP More data received than the available Data Sequence Mapping.
mptcpmoredatarcvdrate	<Double>	Read-only	Rate (/s) counter for mptcptotmoredatarcvd
mptcperrbadmapcondrop	<Double>	Read-only	MPTCP Drop the session incase of invalid Data Sequence map.
mptcperrbadmapcondroprate	<Double>	Read-only	Rate (/s) counter for mptcperrbadmapcondrop
mptcperrdupmaprecvd	<Double>	Read-only	MPTCP Duplicate maps in Data Sequence map table.
mptcperrdupmaprecvdrate	<Double>	Read-only	Rate (/s) counter for mptcperrdupmaprecvd
mptcperrinvalidsfn	<Double>	Read-only	MPTCP subflow map doesn't exactly match MPTCP session mapping.
mptcperrinvalidsfnrate	<Double>	Read-only	Rate (/s) counter for mptcperrinvalidsfn
mptcperrmapexists	<Double>	Read-only	MPTCP sequence map already exists.
mptcperrmapexistsrate	<Double>	Read-only	Rate (/s) counter for mptcperrmapexists

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
mptcperrretxpktrcvd	<Double>	Read-only	Retransmitted Data Recevied on MPTCP session.
mptcperrretxpktrcvdrate	<Double>	Read-only	Rate (/s) counter for mptcperrretxpktrcvd
mptcperrsfsessionallocfail	<Double>	Read-only	Attaching the subflow to MPTCP session failed due to failure in allocating memory to subflow map table.
mptcperrsfsessionallocfailrate	<Double>	Read-only	Rate (/s) counter for mptcperrsfsessionallocfail
mptcperrmpcapsessionallocfail	<Double>	Read-only	Creating a MPTCP connection failed due to failure in allocating memory to MPTCP connection management structure.
mptcperrmpcapsessionallocfailrate	<Double>	Read-only	Rate (/s) counter for mptcperrmpcapsessionallocfail
mptcptotmpcapsfpcballoc	<Double>	Read-only	Allocating memory to TCP protocol control block(PCB) for subflow failed.
mptcpmpcapsfpcballocrate	<Double>	Read-only	Rate (/s) counter for mptcptotmpcapsfpcballoc

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
mptcptotmpcballocfailed	<Double>	Read-only	Allocating memory to MPTCP protocol control block failed.
mptcpmpcballocfailedrate	<Double>	Read-only	Rate (/s) counter for mptcptotmpcballocfailed
mptcperrnsballocfailed	<Double>	Read-only	Failed to allocate memory to output MPTCP packet.
mptcperrnsballocfailedrate	<Double>	Read-only	Rate (/s) counter for mptcperrnsballocfailed
mptcperrnosffreensb	<Double>	Read-only	MPTCP output a packet without any subflow PCB.
mptcperrnosffreensbrate	<Double>	Read-only	Rate (/s) counter for mptcperrnosffreensb
mptcperrv1datarecvdpriortokey	<Double>	Read-only	MPTCP V1 data received prior to key
mptcperrv1datarecvdpriortokeyrate	<Double>	Read-only	Rate (/s) counter for mptcperrv1datarecvdpriortokey

Operations

(click to see Properties)

- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/protocolmptcp **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/protocolmptcp? **args=detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get protocolmptcp resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/protocolmptcp? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "protocolmptcp": [ {

"mptcpmpcapfackrecvdrate":<Double_value>,

"mptcperrremaddrself":<Double_value>,

"mptcptotmpjoinsyn":<Double_value>,

"mptcperrv1datarecvdpriortokey":<Double_value>,

"mptcptotrxdss":<Double_value>,

"mptcpmpcballocfailedrate":<Double_value>,

"mptcperrversionnotsupportedrate":<Double_value>,

"mptcperrretxpktrcvd":<Double_value>,

"mptcperrmaxsfrate":<Double_value>,

"mptcperrinvaloptsrate":<Double_value>,

"mptcpplainackrstrate":<Double_value>,

"mptcperrfastclosekeyrate":<Double_value>,

"mptcptotdssfreshack":<Double_value>,

"mptcperrresflagset":<Double_value>,

"mptcperrfastcloserate":<Double_value>,

"mptcperrv1datarecvdpriortokeyrate":<Double_value>,
```

```
"mptcprxdatafinrate":<Double_value>,

"mptcpestsfreplacedrate":<Double_value>,

"mptcpplainackrst":<Double_value>,

"mptcpprioclearbackuprxrate":<Double_value>,

"mptcperrdupmaprecvd":<Double_value>,

"mptcptotv1mpcapsession":<Double_value>,

"mptcptottxdss":<Double_value>,

"mptcperroptiondiscardedrate":<Double_value>,

"mptcptotfreshackfrwd":<Double_value>,

"mptcpaddrremovedrate":<Double_value>,

"mptcptxdssrate":<Double_value>,

"mptcperrfastclosepassive":<Double_value>,

"mptcperrjointhresholdrate":<Double_value>,

"mptcperrfastclosekey":<Double_value>,

"mptcpmpjoinsteeredrate":<Double_value>,

"mptcpmpfailsentrate":<Double_value>,

"mptcptotmpcapsteered":<Double_value>,

"mptcperraddrid0rate":<Double_value>,

"mptcperrnosffreensbrate":<Double_value>,

"mptcpinfinitemaprecvd":<Double_value>,

"mptcperrbadmapconndroprate":<Double_value>,

"mptcperroptsnosessionrate":<Double_value>,
```

```
"mptcperrjoinafterfallback":<Double_value>,

"mptcpplainackfallback":<Double_value>,

"mptcptottxsffin":<Double_value>,

"mptcperrinvalopts":<Double_value>,

"mptcperrfastclose":<Double_value>,

"mptcperroptssendrstrate":<Double_value>,

"mptcperrmpcapsessionallocfail":<Double_value>,

"mptcpdssmrate":<Double_value>,

"mptcptotmpjoinsteered":<Double_value>,

"mptcperrinvalmacrate":<Double_value>,

"mptcptotpendsfreplaced":<Double_value>,

"mptcperroptiondiscarded":<Double_value>,

"mptcperroptsnosession":<Double_value>,

"mptcperrbadmapconndrop":<Double_value>,

"mptcpmpcapsfpcballocrate":<Double_value>,

"mptcpcursesswithoutsfs":<Double_value>,

"mptcperrinvalmac":<Double_value>,

"mptcpprioclearbackuprx":<Double_value>,

"mptcptotmpjoinfackrecvd":<Double_value>,

"mptcperrinvalcookierate":<Double_value>,

"mptcptotconnest":<Double_value>,

"mptcpdssfreshackrate":<Double_value>,
```

```
"mptcpdssrate":<Double_value>,

"mptcperrunsupportedmssnegotiatedrate":<Double_value>,

"mptcperrinvalidsfnrate":<Double_value>,

"mptcperrrssffailrate":<Double_value>,

"mptcperrextnflagset":<Double_value>,

"mptcperraddridexistrate":<Double_value>,

"mptcperrrssffail":<Double_value>,

"mptcpdatalessthandatalenrate":<Double_value>,

"mptcptotmpcapsynacksent":<Double_value>,

"mptcpcurmpcapablesessions":<Double_value>,

"mptcpsfconnrate":<Double_value>,

"mptcpinfinitemaprecvdrate":<Double_value>,

"mptcpmpjoinsynrate":<Double_value>,

"mptcptotmpcapsyn":<Double_value>,

"mptcperraddrid0":<Double_value>,

"mptcpmpjoin4thacksentrate":<Double_value>,

"mptcptotdss":<Double_value>,

"mptcpmoredatarcvdrate":<Double_value>,

"mptcperrinvalcookie":<Double_value>,

"mptcpmpfailsent":<Double_value>,

"mptcpmpcapsessionrate":<Double_value>,

"mptcpcurpendingjoin":<Double_value>,
```

```
"mptcptotmpcballocfailed":<Double_value>,

"mptcperrdatafinpassive":<Double_value>,

"mptcperrsfsessionallocfail":<Double_value>,

"mptcpinfinitemapfrwdrate":<Double_value>,

"mptcperrnopayloadlenpkt":<Double_value>,

"mptcperrmpcapsessionallocfailrate":<Double_value>,

"mptcpcurv1mpcapablesessions":<Double_value>,

"mptcpmpjoinsynacksentrate":<Double_value>,

"mptcperrunknowntoken":<Double_value>,

"mptcperrcryptonotsupportedrate":<Double_value>,

"mptcperrfastclosepassiverate":<Double_value>,

"mptcperroptssendrst":<Double_value>,

"mptcppriobackuprxrate":<Double_value>,

"mptcptotinfinitemapfrwd":<Double_value>,

"mptcperrresflagsetrate":<Double_value>,

"mptcptotmpcapfackrecvd":<Double_value>,

"mptcpv1mpcapsynrate":<Double_value>,

"mptcperrunknowntokenrate":<Double_value>,

"mptcperrjointhreshold":<Double_value>,

"mptcpdssarate":<Double_value>,

"mptcperrnopayloadlenpktrate":<Double_value>,

"mptcptotmpcapsession":<Double_value>,
```

```
"mptcpfreshackfrwdrate":<Double_value>,

"mptcptotmoredatarcvd":<Double_value>,

"mptcpplainackfallbackrate":<Double_value>,

"mptcptotdssm":<Double_value>,

"mptcperraddridexist":<Double_value>,

"mptcperrextnflagsetrate":<Double_value>,

"mptcppendsfreplacedrate":<Double_value>,

"mptcperrmapexists":<Double_value>,

"mptcperrbadcksum":<Double_value>,

"mptcptotestsfreplaced":<Double_value>,

"mptcptxsffinrate":<Double_value>,

"mptcperrdatafinpassiverate":<Double_value>,

"mptcpmpcapsteeredrate":<Double_value>,

"mptcperrbadcksumrate":<Double_value>,

"mptcpmpcapsynacksentrate":<Double_value>,

"mptcperrinvalremaddrrate":<Double_value>,

"mptcptotv1mpcapsyn":<Double_value>,

"mptcperrnomappktrcvdrate":<Double_value>,

"mptcppriobackuprx":<Double_value>,

"mptcptotsfconn":<Double_value>,

"mptcperrunsupportedmssnegotiated":<Double_value>,

"mptcprxdssrate":<Double_value>,
```

```
"mptcperrretxpktrcvdrate":<Double_value>,

"mptcpv1mpcapsessionrate":<Double_value>,

"mptcptotmpjoinsynacksent":<Double_value>,

"mptcptotdatalessthandatalen":<Double_value>,

"mptcperrversionnotsupported":<Double_value>,

"mptcptotmpcapsfpcballoc":<Double_value>,

"mptcptotaddrremoved":<Double_value>,

"mptcptottxdatafin":<Double_value>,

"mptcperrremaddrselfrate":<Double_value>,

"mptcperrmaxsf":<Double_value>,

"mptcpcursfconnections":<Double_value>,

"mptcperrmapexistsrate":<Double_value>,

"mptcperrnosffreensb":<Double_value>,

"mptcperrsfsessionallocfailrate":<Double_value>,

"mptcptotmpjoin4thacksent":<Double_value>,

"mptcperrcryptonotsupported":<Double_value>,

"mptcperrinvalidsfn":<Double_value>,

"mptcperrjoinafterfallbackrate":<Double_value>,

"mptcperrnsballocfailed":<Double_value>,

"mptcpconnestrate":<Double_value>,

"mptcptotdssa":<Double_value>,

"mptcpmpfailrecvdrate":<Double_value>,
```

```
"mptcperrnsballocfailedrate":<Double_value>,

"mptcpmpfailrecvd":<Double_value>,

"mptcperrinvalremaddr":<Double_value>,

"mptcptotrxdatafin":<Double_value>,

"mptcptxdatafinrate":<Double_value>,

"mptcpmpcapsynrate":<Double_value>,

"mptcperrnomappktrcvd":<Double_value>,

"mptcpmpjoinfackrecvdrate":<Double_value>,

"mptcperrdupmaprecvdrate":<Double_value>

}]}
```

protocolquic

Statistics for QUIC protocol resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full
quicclientdgrmrcvd	<Double>	Read-only	Total QUIC client UDP datagrams received
quicclientdgrmrcvdrate	<Double>	Read-only	Rate (/s) counter for quicclientdgrmrcvd

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
quicserverdgrmrcvd	<Double>	Read-only	Total QUIC server UDP datagrams received
quicserverdgrmrcvdrate	<Double>	Read-only	Rate (/s) counter for quicserverdgrmrcvd
quicclientdgrmsent	<Double>	Read-only	Total QUIC client UDP datagrams sent
quicclientdgrmsentrate	<Double>	Read-only	Rate (/s) counter for quicclientdgrmsent
quicserverdgrmsent	<Double>	Read-only	Total QUIC server UDP datagrams sent
quicserverdgrmsentrate	<Double>	Read-only	Rate (/s) counter for quicserverdgrmsent
quiccurclientconn	<Double>	Read-only	Current QUIC client connections
quiccurclientconnrate	<Double>	Read-only	Rate (/s) counter for quiccurclientconn
quiccurserverconn	<Double>	Read-only	Current QUIC server connections
quiccurserverconnrate	<Double>	Read-only	Rate (/s) counter for quiccurserverconn
quiclocalconnid	<Double>	Read-only	Current QUIC local connection IDs allocated
quiclocalconnidrate	<Double>	Read-only	Rate (/s) counter for quiclocalconnid
quiccursavedcryptoctx	<Double>	Read-only	Current QUIC crypto contexts allocated

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
quiccursavedcryptoctxrate	<Double>	Read-only	Rate (/s) counter for quiccursavedcryptoctx
quictotclientconn	<Double>	Read-only	Total QUIC client connections
quicclientconnrate	<Double>	Read-only	Rate (/s) counter for quictotclientconn
quictotserverconn	<Double>	Read-only	Total QUIC server connections
quicserverconnrate	<Double>	Read-only	Rate (/s) counter for quictotserverconn
quicmigratedconn	<Double>	Read-only	Total number of migrated QUIC connections
quicmigratedconnrate	<Double>	Read-only	Rate (/s) counter for quicmigratedconn
quicjumboframesrcvd	<Double>	Read-only	Total number of QUIC jumbo frames received
quicjumboframesrcvdrate	<Double>	Read-only	Rate (/s) counter for quicjumboframesrcvd
quicretrypktsent	<Double>	Read-only	Number of QUIC Retry packets sent
quicretrypktsentrate	<Double>	Read-only	Rate (/s) counter for quicretrypktsent
quichandshakecmpltd	<Double>	Read-only	Number of QUIC handshake messages completed

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
quichandshakecmpltdrate	<Double>	Read-only	Rate (/s) counter for quichandshakecmpltd
quictransptconncloseptsent	<Double>	Read-only	Number of QUIC transport no-error Connection Close packets sent
quictransptconncloseptsentrate	<Double>	Read-only	Rate (/s) counter for quictransptconncloseptsent
quicappconnclosepktsent	<Double>	Read-only	Number of QUIC application no-error Connection Close packets sent
quicappconnclosepktsentrate	<Double>	Read-only	Rate (/s) counter for quicappconnclosepktsent
quicasyncdatagramssent	<Double>	Read-only	Number of QUIC datagrams sent using async mode
quicasyncdatagramssentrate	<Double>	Read-only	Rate (/s) counter for quicasyncdatagramssent
quicconninfoalcfail	<Double>	Read-only	Quic session allocations failed
quicconninfoalcfailrate	<Double>	Read-only	Rate (/s) counter for quicconninfoalcfail
quicnsbalcfail	<Double>	Read-only	Quic NSB allocations failed
quicnsbalcfailrate	<Double>	Read-only	Rate (/s) counter for quicnsbalcfail

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
quictlsalertsent	<Double>	Read-only	Total QUIC TLS 1.3 transport errors sent
quictlsalertsentrate	<Double>	Read-only	Rate (/s) counter for quictlsalertsent
quicstlessconnclosepktsent	<Double>	Read-only	Number of QUIC stateless Connection Close packets sent
quicstlessconnclosepktsentrate	<Double>	Read-only	Rate (/s) counter for quicstlessconnclosepktsent
quicvernegpktsent	<Double>	Read-only	Number of QUIC Version Negotiation packets sent
quicvernegpktsentrate	<Double>	Read-only	Rate (/s) counter for quicvernegpktsent
quictransptconnclosepktfail	<Double>	Read-only	Number of QUIC transport error Connection Close packets sent
quictransptconnclosepktfailrate	<Double>	Read-only	Rate (/s) counter for quictransptconnclosepktfail
quicappconnclosepktfail	<Double>	Read-only	Number of QUIC application error Connection Close packets sent
quicappconnclosepktfailrate	<Double>	Read-only	Rate (/s) counter for quicappconnclosepktfail

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
quicretrytokenverfail	<Double>	Read-only	Number of times QUIC Retry token verification failed
quicretrytokenverfailrate	<Double>	Read-only	Rate (/s) counter for quicretrytokenverfail
quicnewtokenverfail	<Double>	Read-only	Number of times QUIC NEW_TOKEN token verification failed
quicnewtokenverfailrate	<Double>	Read-only	Rate (/s) counter for quicnewtokenverfail

Operations

(click to see Properties)

- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/protocolquic **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/protocolquic? **args=detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get protocolquic resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/protocolquic? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "protocolquic": [ {

"quicretrytokenverfail":<Double_value>,

"quiccurclientconnrate":<Double_value>,
```

```
"quicserverdgrmrcvdrate":<Double_value>,

"quiclocalconnid":<Double_value>,

"quichandshakecmpltd":<Double_value>,

"quicappconnclosepktsent":<Double_value>,

"quicconninfoalcfailrate":<Double_value>,

"quicvernegpktsent":<Double_value>,

"quictotclientconn":<Double_value>,

"quicclientdgrmrcvdrate":<Double_value>,

"quicnewtokenverfail":<Double_value>,

"quicclientdgrmsentrate":<Double_value>,

"quicvernegpktsentrate":<Double_value>,

"quictransptconnclosepktfail":<Double_value>,

"quiccurclientconn":<Double_value>,

"quicappconnclosepktfailrate":<Double_value>,

"quicretrypktsentrate":<Double_value>,

"quictlsalertsentrate":<Double_value>,

"quictlsalertsent":<Double_value>,

"quicretrypktsent":<Double_value>,

"quicjumboframesrcvdrate":<Double_value>,

"quicasyncdatagramssent":<Double_value>,

"quicserverdgrmsentrate":<Double_value>,

"quicserverconnrate":<Double_value>,
```

```
"quicappconnclosepktfail":<Double_value>,

"quiccursavedcryptoctxrate":<Double_value>,

"quicserverdgrmrcvd":<Double_value>,

"quictotserverconn":<Double_value>,

"quicnsbalcfail":<Double_value>,

"quicretrytokenverfailrate":<Double_value>,

"quictransptconnclosepktsentrate":<Double_value>,

"quiclocalconnidrate":<Double_value>,

"quicmigratedconn":<Double_value>,

"quicjumboframesrcvd":<Double_value>,

"quicclientconnrate":<Double_value>,

"quictransptconnclosepktfailrate":<Double_value>,

"quicclientdgrmrcvd":<Double_value>,

"quictransptconnclosepktsent":<Double_value>,

"quicmigratedconnrate":<Double_value>,

"quiccurserverconnrate":<Double_value>,

"quicstlessconnclosepktsent":<Double_value>,

"quicconninfoalcfail":<Double_value>,

"quicclientdgrmsent":<Double_value>,

"quichandshakecmpltdrate":<Double_value>,

"quicasyncdatagramssentrate":<Double_value>,

"quicstlessconnclosepktsentrate":<Double_value>,
```

```
"quicnewtokenverfailrate":<Double_value>,

"quicappconnclosepktsentrate":<Double_value>,

"quiccursavedcryptoctx":<Double_value>,

"quiccurserverconn":<Double_value>,

"quicnsbalcfailrate":<Double_value>,

"quicserverdgrmsent":<Double_value>

}]}
```

protocolquicbridge

Statistics for QUIC Bridge protocol resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full
quicbridgeconn	<Double>	Read-only	Total number of QUIC Bridge connections
quicbridgeconnrate	<Double>	Read-only	Rate (/s) counter for quicbridgeconn
quicbridgemigratedconn	<Double>	Read-only	Total number of migrated QUIC Bridge connections

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
quicbridgemigratedconnrate	<Double>	Read-only	Rate (/s) counter for quicbridgemigratedconn
quicbridgeqci	<Double>	Read-only	Current number of QUIC Bridge connection infos
quicbridgeqcirate	<Double>	Read-only	Rate (/s) counter for quicbridgeqci
quicbridgeqpi	<Double>	Read-only	Current number of QUIC Bridge peer infos
quicbridgeqpirate	<Double>	Read-only	Rate (/s) counter for quicbridgeqpi
quicbridgeqpialcfail	<Double>	Read-only	Number of QUIC Bridge peer info allocation failures
quicbridgeqpialcfailrate	<Double>	Read-only	Rate (/s) counter for quicbridgeqpialcfail
quicbridgeqcialcfail	<Double>	Read-only	Number of QUIC Bridge connection info allocation failures
quicbridgeqcialcfailrate	<Double>	Read-only	Rate (/s) counter for quicbridgeqcialcfail

Operations

(click to see Properties)

- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/protocolquicbridge **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/protocolquicbridge? **args=detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get protocolquicbridge resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/protocolquicbridge? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "protocolquicbridge": [ {

"quicbridgeqpialcfail":<Double_value>,

"quicbridgeqci":<Double_value>,

"quicbridgeqpialcfailrate":<Double_value>,

"quicbridgeconn":<Double_value>,

"quicbridgemigratedconnrate":<Double_value>,

"quicbridgeconnrate":<Double_value>,

"quicbridgeqpirate":<Double_value>,

"quicbridgemigratedconn":<Double_value>,

"quicbridgeqcialcfail":<Double_value>,

"quicbridgeqpi":<Double_value>,

"quicbridgeqcialcfailrate":<Double_value>,

"quicbridgeqcirate":<Double_value>

}]}
```

protocoltcp

Statistics for tcp protocol resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full
tcpactiveserverconn	<Double>	Read-only	Connections to a server currently responding to requests.
tcpcurserverconnopening	<Double>	Read-only	Server connections in the Opening state, which indicates that the handshakes are not yet complete.
tcpcurclientconnopening	<Double>	Read-only	Client connections in the Opening state, which indicates that the handshakes are not yet complete.
tcpcurclientconnestablished	<Double>	Read-only	Current client connections in the Established state, which indicates that data transfer can occur between the Citrix ADC and the client.
tcpcurserverconnestablished	<Double>	Read-only	Current server connections in the Established state,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			which indicates that data transfer can occur between the Citrix ADC and the server.
tcptotrxpkts	<Double>	Read-only	TCP packets received.
tcprxpktsrate	<Double>	Read-only	Rate (/s) counter for tcptotrxpkts
tcptotrxbytes	<Double>	Read-only	Bytes of TCP data received.
tcprxbytesrate	<Double>	Read-only	Rate (/s) counter for tcptotrxbytes
tcptottxpkts	<Double>	Read-only	TCP packets transmitted.
tcptxpktsrate	<Double>	Read-only	Rate (/s) counter for tcptottxpkts
tcptottxbytes	<Double>	Read-only	Bytes of TCP data transmitted.
tcptxbytesrate	<Double>	Read-only	Rate (/s) counter for tcptottxbytes
tcpcurclientconn	<Double>	Read-only	Client connections, including connections in the Opening, Established, and Closing state.
tcpcurclientconnclosing	<Double>	Read-only	Client connections in the Closing state, which indicates that the connection termination process

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			has initiated but is not complete.
tcptotclientconnopened	<Double>	Read-only	Client connections opened by the Citrix ADC since startup (after three-way handshake). This counter is reset when the Citrix ADC is restarted.
tcpclientconnopenedrate	<Double>	Read-only	Rate (/s) counter for tcptotclientconnopened
tcpcurserverconn	<Double>	Read-only	Server connections, including connections in the Opening, Established, and Closing state.
tcpcurserverconnclosing	<Double>	Read-only	Server connections in the Closing state, which indicates that the connection termination process has initiated but is not complete.
tcptotserverconnopened	<Double>	Read-only	Server connections initiated by the Citrix ADC since startup. This counter is reset when the Citrix ADC is restarted.
tcpserverconnopenedrate	<Double>	Read-only	Rate (/s) counter for tcptotserverconnopened

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
tcpsurgequeuelen	<Double>	Read-only	Connections in the surge queue. When the Citrix ADC cannot open a connection to the server, for example when maximum connections have been reached, the Citrix ADC queues these requests.
tcpspareconn	<Double>	Read-only	Spare connections available. To save time and resources in establishing another connection for a new client, the connection on the server is not closed after completing the request from the first client and is available for serving future requests.
tcptotzombiecltconnflushed	<Double>	Read-only	Client connections that are flushed because the client has been idle for some time.
tcpzombiecltconnflushedrate	<Double>	Read-only	Rate (/s) counter for tcptotzombiecltconnflushed
tcptotzombiehalfopencltconnflushed	<Double>	Read-only	Half-opened client connections that are flushed because the three-way

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			handshakes are not complete.
tcpzombiehalfopencltconnflushedrate	<Double>	Read-only	Rate (/s) counter for tcptotzombiehalfopencltconnflushed
tcptotzombieactivehalfclosecltconnflushed	<Double>	Read-only	Active half-closed client connections that are flushed because the client has closed the connection and there has been no activity on the connection.
tcpzombieactivehalfclosecltconnflushedrate	<Double>	Read-only	Rate (/s) counter for tcptotzombieactivehalfclosecltconnflushed
tcptotzombiepassivehalfclosecltconnflushed	<Double>	Read-only	Passive half-closed client connections that are flushed because the Citrix ADC has closed the connection and there has been no activity on the connection.
tcpzombiepassivehalfclosecltconnflushedrate	<Double>	Read-only	Rate (/s) counter for tcptotzombiepassivehalfclosecltconnflushed
tcptotzombiesvrconnflushed	<Double>	Read-only	Server connections that are flushed because there have been no client requests in the queue for some time.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
tcpzombiesvrconnflushedrate	<Double>	Read-only	Rate (/s) counter for tcptotzombiesvrconnflushed
tcptotzombiehalfopensvrconnflushed	<Double>	Read-only	Half-opened server connections that are flushed because the three-way handshakes are not complete.
tcpzombiehalfopensvrconnflushedrate	<Double>	Read-only	Rate (/s) counter for tcptotzombiehalfopensvrconnflushed
tcptotzombieactivehalfclosesvrconnflushed	<Double>	Read-only	Active half-closed server connections that are flushed because the server has closed the connection and there has been no activity on the connection.
tcpzombieactivehalfclosesvrconnflushedrate	<Double>	Read-only	Rate (/s) counter for tcptotzombieactivehalfclosesvrconnflushed
tcptotzombiepassivehalfclosesrvconnflushed	<Double>	Read-only	Passive half-closed server connections that are flushed because the Citrix ADC has closed the connection and there has been no activity on the connection.
tcpzombiepassivehalfclosesrvconnflushedrate	<Double>	Read-only	Rate (/s) counter for tcptotzombiepassive

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			halfclosesrvconnflushed
pcbtotzombiecall	<Double>	Read-only	Times the Zombie cleanup function is called. Every time a connection is flushed, it is marked for cleanup. The Zombie cleanup function clears all these connections at predefined intervals.
pcbzombiecallrate	<Double>	Read-only	Rate (/s) counter for pcbtotzombiecall
tcptotsyn	<Double>	Read-only	SYN packets received
tcpsynrate	<Double>	Read-only	Rate (/s) counter for tcptotsyn
tcptotsynprobe	<Double>	Read-only	Probes from the Citrix ADC to a server. The Citrix ADC sends a SYN packet to the server to check its availability and expects a SYN_ACK packet from the server before a specified response timeout.
tcpsynproberate	<Double>	Read-only	Rate (/s) counter for tcptotsynprobe
tcptotsvrfin	<Double>	Read-only	FIN packets received from the server.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
tcpsvrfinrate	<Double>	Read-only	Rate (/s) counter for tcptotsvrfin
tcptotcltfin	<Double>	Read-only	FIN packets received from the clients.
tcpcltfinrate	<Double>	Read-only	Rate (/s) counter for tcptotcltfin
tcpwaittosyn	<Double>	Read-only	SYN packets (packets used to initiate a TCP connection) received on connections that are in the TIME_WAIT state. Packets cannot be transferred on a connection in this state.
tcpwaittosynrate	<Double>	Read-only	Rate (/s) counter for tcpwaittosyn
tcpwaittodata	<Double>	Read-only	Bytes of data received on connections that are in the TIME_WAIT state. Data cannot be transferred on a connection that is in this state.
tcpwaittodatarate	<Double>	Read-only	Rate (/s) counter for tcpwaittodata
tcptotsynheld	<Double>	Read-only	SYN packets held on the Citrix ADC that are waiting for a server connection.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
tcpsynheldrate	<Double>	Read-only	Rate (/s) counter for tcptotsynheld
tcptotsynflush	<Double>	Read-only	SYN packets flushed on the Citrix ADC because of no response from the server for three or more seconds.
tcpsynflushrate	<Double>	Read-only	Rate (/s) counter for tcptotsynflush
tcptotfinwaitclosed	<Double>	Read-only	Connections closed on the Citrix ADC because the number of connections in the TIME_WAIT state has exceeded the default value of 7000.
tcpfinwaitclosedrate	<Double>	Read-only	Rate (/s) counter for tcptotfinwaitclosed
tcperrbadchecksum	<Double>	Read-only	Packets received with a TCP checksum error.
tcperrbadchecksumrate	<Double>	Read-only	Rate (/s) counter for tcperrbadchecksum
tcperrdataafterfin	<Double>	Read-only	Packets received following a connection termination request. This error is usually caused by a reordering of packets during transmission.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
tcperrdataafterfinrate	<Double>	Read-only	Rate (/s) counter for tcperrdataafterfin
tcperrsyninsynrcvd	<Double>	Read-only	SYN packets received on a connection that is in the SYN_RCVD state. A connection goes into the SYN_RCVD state after receiving a SYN packet.
tcperrsyninsynrcvdrate	<Double>	Read-only	Rate (/s) counter for tcperrsyninsynrcvd
tcperrsyninest	<Double>	Read-only	SYN packets received on a connection that is in the ESTABLISHED state. A SYN packet is not expected on an ESTABLISHED connection.
tcperrsyninestrate	<Double>	Read-only	Rate (/s) counter for tcperrsyninest
tcperrsynsentbadack	<Double>	Read-only	Incorrect ACK packets received on a connection that is in the SYN_SENT state. An incorrect ACK packet is the third packet in the three-way handshake that has an incorrect sequence number.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
tcperrsynsentbadackrate	<Double>	Read-only	Rate (/s) counter for tcperrsynsentbadack
tcperrrst	<Double>	Read-only	Reset packets received from a client or a server.
tcperrrstrate	<Double>	Read-only	Rate (/s) counter for tcperrrst
tcperrrstnonest	<Double>	Read-only	Reset packets received on a connection that is not in the ESTABLISHED state.
tcperrrstnonestrate	<Double>	Read-only	Rate (/s) counter for tcperrrstnonest
tcperrrstoutofwindow	<Double>	Read-only	Reset packets received on a connection that is out of the current TCP window.
tcperrrstoutofwindowrate	<Double>	Read-only	Rate (/s) counter for tcperrrstoutofwindow
tcperrrstintimewait	<Double>	Read-only	Reset packets received on a connection that is in the TIME_WAIT state. Packets cannot be transferred on a connection in the TIME_WAIT state.
tcperrrstintimewaitrate	<Double>	Read-only	Rate (/s) counter for tcperrrstintimewait

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
tcperrsvroutoforder	<Double>	Read-only	Out of order TCP packets received from a server.
tcperrsvroutoforderrate	<Double>	Read-only	Rate (/s) counter for tcperrsvroutoforder
tcperrcltoutoforder	<Double>	Read-only	Out of order TCP packets received from a client.
tcperrcltoutoforderrate	<Double>	Read-only	Rate (/s) counter for tcperrcltoutoforder
tcperrclthole	<Double>	Read-only	TCP holes created on a client connection. When out of order packets are received from a client, a hole is created on the Citrix ADC for each group of missing packets.
tcperrcltholerate	<Double>	Read-only	Rate (/s) counter for tcperrclthole
tcperrsvrhole	<Double>	Read-only	TCP holes created on a server connection. When out of order packets are received from a server, a hole is created on the Citrix ADC for each group of missing packets.
tcperrsvrholerate	<Double>	Read-only	Rate (/s) counter for tcperrsvrhole

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
tcperrcookiepktseqreject	<Double>	Read-only	SYN cookie packets rejected because they contain an incorrect sequence number.
tcperrcookiepktseqrejectrate	<Double>	Read-only	Rate (/s) counter for tcperrcookiepktseqreject
tcperrcookiepktsigreject	<Double>	Read-only	SYN cookie packets rejected because they contain an incorrect signature.
tcperrcookiepktsigrejectrate	<Double>	Read-only	Rate (/s) counter for tcperrcookiepktsigreject
tcperrcookiepktseqdrop	<Double>	Read-only	SYN cookie packets dropped because the sequence number specified in the packets is outside the current window.
tcperrcookiepktseqdroprate	<Double>	Read-only	Rate (/s) counter for tcperrcookiepktseqdrop
tcperrcookiepktmssreject	<Double>	Read-only	SYN cookie packets rejected because the maximum segment size (MSS) specified in the packets is incorrect.
tcperrcookiepktmssrejectrate	<Double>	Read-only	Rate (/s) counter for tcperrcookiepktmssreject

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
tcperranyportfail	<Double>	Read-only	Port allocations that have failed on a mapped IP address because the maximum limit of 65536 has been exceeded.
tcperranyportfailrate	<Double>	Read-only	Rate (/s) counter for tcperranyportfail
tcperripportfail	<Double>	Read-only	Port allocations that have failed on a subnet IP address or vserver IP address because the maximum limit of 65536 has been exceeded.
tcperripportfailrate	<Double>	Read-only	Rate (/s) counter for tcperripportfail
tcperrstraypkt	<Double>	Read-only	Number of stray or misrouted packets.
tcperrstraypktrate	<Double>	Read-only	Rate (/s) counter for tcperrstraypkt
tcperrsentrst	<Double>	Read-only	Reset packets sent to a client or a server.
tcperrsentrstrate	<Double>	Read-only	Rate (/s) counter for tcperrsentrst
tcperrbadstateconn	<Double>	Read-only	Connections that are not in a valid TCP state.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
tcperrbadstateconnrate	<Double>	Read-only	Rate (/s) counter for tcperrbadstateconn
tcperrrstthreshold	<Double>	Read-only	Reset packets dropped because the default threshold of 100 resets per 10 milliseconds has been exceeded. This is a configurable value using the set rateControl command.
tcperrrstthresholdrate	<Double>	Read-only	Rate (/s) counter for tcperrrstthreshold
tcperroutofwindowpkts	<Double>	Read-only	Packets received that are out of the current advertised window.
tcperroutofwindowpktsrate	<Double>	Read-only	Rate (/s) counter for tcperroutofwindowpkts
tcperrsyndroppedcongestion	<Double>	Read-only	SYN packets dropped because of network congestion.
tcperrsyndroppedcongestionrate	<Double>	Read-only	Rate (/s) counter for tcperrsyndroppedcongestion
tcperrcltretrasmit	<Double>	Read-only	Packets retransmitted by a client. This usually occurs because the acknowledgement from the Citrix ADC

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			has not reached the client.
tcperrcltretrasmitrate	<Double>	Read-only	Rate (/s) counter for tcperrcltretrasmit
tcperrfullretrasmit	<Double>	Read-only	Full packets retransmitted by the client or the server.
tcperrfullretrasmitrate	<Double>	Read-only	Rate (/s) counter for tcperrfullretrasmit
tcperrsynretry	<Double>	Read-only	SYN packets resent to a server.
tcperrsynretryrate	<Double>	Read-only	Rate (/s) counter for tcperrsynretry
tcperrsyngiveup	<Double>	Read-only	Attempts to establish a connection on the Citrix ADC that timed out.
tcperrsyngiveuprate	<Double>	Read-only	Rate (/s) counter for tcperrsyngiveup
tcperrretransmit	<Double>	Read-only	TCP packets retransmitted. The Citrix ADC attempts to retransmit the packet up to seven times, after which it resets the other half of the TCP connection.
tcperrretransmitrate	<Double>	Read-only	Rate (/s) counter for tcperrretransmit

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
tcperrfirstretransmissions	<Double>	Read-only	Packets retransmitted once by the Citrix ADC.
tcperrfirstretransmissionsrate	<Double>	Read-only	Rate (/s) counter for tcperrfirstretransmissions
tcperrthirdretransmissions	<Double>	Read-only	Packets retransmitted three times by the Citrix ADC.
tcperrthirdretransmissionsrate	<Double>	Read-only	Rate (/s) counter for tcperrthirdretransmissions
tcperrfifthretransmissions	<Double>	Read-only	Packets retransmitted five times by the Citrix ADC.
tcperrfifthretransmissionsrate	<Double>	Read-only	Rate (/s) counter for tcperrfifthretransmissions
tcperrseventhretransmissions	<Double>	Read-only	Packets retransmitted seven times by the Citrix ADC. If this fails, the Citrix ADC terminates the connection.
tcperrseventhretransmissionsrate	<Double>	Read-only	Rate (/s) counter for tcperrseventhretransmissions
tcperrfastretransmissions	<Double>	Read-only	TCP packets on which the Citrix ADC performs a fast

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			retransmission in response to three duplicate acknowledgements or a partial acknowledgement. The Citrix ADC assumes that the packet is lost and retransmits the packet before its time-out.
tcperrfastretransmissionsrate	<Double>	Read-only	Rate (/s) counter for tcperrfastretransmissions
tcperrsvrretrasmit	<Double>	Read-only	Packets retransmitted by a server. This usually occurs because the acknowledgement from the Citrix ADC has not reached the server.
tcperrsvrretrasmitrate	<Double>	Read-only	Rate (/s) counter for tcperrsvrretrasmit
tcperrpartialretrasmit	<Double>	Read-only	Partial packet retransmits by a client or server due to congestion on the connection. This usually occurs because the window advertised by the Citrix ADC is not big enough to hold the full packet.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
tcperrpartialretrasmit rate	<Double>	Read-only	Rate (/s) counter for tcperrpartialretrasmit
tcperrfinretry	<Double>	Read-only	FIN packets resent to a server or a client.
tcperrfinretryrate	<Double>	Read-only	Rate (/s) counter for tcperrfinretry
tcperrfingiveup	<Double>	Read-only	Connections that were timed out by the Citrix ADC because of not receiving the ACK packet after retransmitting the FIN packet four times.
tcperrfingiveuprate	<Double>	Read-only	Rate (/s) counter for tcperrfingiveup
tcperrsecondretrans missions	<Double>	Read-only	Packets retransmitted twice by the Citrix ADC.
tcperrsecondretrans missionsrate	<Double>	Read-only	Rate (/s) counter for tcperrsecondretrans missions
tcperrforthretransmis sions	<Double>	Read-only	Packets retransmitted four times by the Citrix ADC.
tcperrforthretransmis sionsrate	<Double>	Read-only	Rate (/s) counter for tcperrforthretransmis sions

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
tcperrsixthretransmissions	<Double>	Read-only	Packets retransmitted six times by the Citrix ADC.
tcperrsixthretransmissionsrate	<Double>	Read-only	Rate (/s) counter for tcperrsixthretransmissions
tcperrretransmitgiveup	<Double>	Read-only	Number of times Citrix ADC terminates a connection after retransmitting the packet seven times on that connection.Retrasnmission happens when recieving end doesn't acknowledges the packet.
tcperrretransmitgiveuprate	<Double>	Read-only	Rate (/s) counter for tcperrretransmitgiveup
tcperrcipalloc	<Double>	Read-only	Number of times TCP level client header insertion failure
tcperrcipallocrate	<Double>	Read-only	Rate (/s) counter for tcperrcipalloc

Operations

(click to see Properties)

- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/protocoltcp **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/protocoltcp? **args=detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get protocoltcp resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/protocoltcp? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "protocoltcp": [ {

"tcperrseventhretransmissionsrate":<Double_value>,

"tcptottxpkts":<Double_value>,

"tcperrfinretryrate":<Double_value>,

"tcperrcltoutoforderrate":<Double_value>,

"tcperrdataafterfin":<Double_value>,

"tcperrsvrhole":<Double_value>,

"tcperrsyngiveuprate":<Double_value>,

"tcptotcltfin":<Double_value>,

"tcpcltfinrate":<Double_value>,

"tcperrsixthretransmissions":<Double_value>,

"tcperrstraypkt":<Double_value>,

"tcptotsvrfin":<Double_value>,

"tcptotsynprobe":<Double_value>,

"tcptotzombiesvrconnflushed":<Double_value>,

"tcperrsyndroppedcongestion":<Double_value>,
```

```
"tcperrfullretrasmit":<Double_value>,

"tcperrclthole":<Double_value>,

"tcperrrstthresholdrate":<Double_value>,

"tcperrcookiepktsigrejectrate":<Double_value>,

"tcperrfirstretransmissionsrate":<Double_value>,

"tcpwaittodatarate":<Double_value>,

"tcperrcookiepktsigreject":<Double_value>,

"tcperrsentrst":<Double_value>,

"tcperrrstnonest":<Double_value>,

"tcptotclientconnopened":<Double_value>,

"tcperrbadstateconnrate":<Double_value>,

"tcpzombiehalfopencltconnflushedrate":<Double_value>,

"tcperrfirstretransmissions":<Double_value>,

"tcperrsvroutoforderrate":<Double_value>,

"tcperrcookiepktseqdroprate":<Double_value>,

"tcperrstraypktrate":<Double_value>,

"tcperrcookiepktmssrejectrate":<Double_value>,

"tcpzombiepassivehalfclosecltconnflushedrate":<Double_value>,

"tcpcurclientconn":<Double_value>,

"tcperrsvrretrasmitrate":<Double_value>,

"tcperrcookiepktseqrejectrate":<Double_value>,

"tcperrfifthretransmissionsrate":<Double_value>,
```

```
"tcperrfingiveup":<Double_value>,

"tcperrpartialretrasmitrate":<Double_value>,

"tcperrsyninsynrcvdrate":<Double_value>,

"tcperrforthretransmissionsrate":<Double_value>,

"tcpzombiesvrconnflushedrate":<Double_value>,

"tcptotzombiehalfopencltconnflushed":<Double_value>,

"tcperrthirdretransmissions":<Double_value>,

"tcperroutofwindowpkts":<Double_value>,

"tcperrseventhretransmissions":<Double_value>,

"tcptotzombieactivehalfclosecltconnflushed":<Double_value>,

"tcptotrxbytes":<Double_value>,

"tcperrsecondretransmissions":<Double_value>,

"tcpactiveserverconn":<Double_value>,

"tcperrfinretry":<Double_value>,

"tcpsynheldrate":<Double_value>,

"tcptotsyn":<Double_value>,

"tcptotzombiehalfopensvrconnflushed":<Double_value>,

"tcpzombieactivehalfclosesvrconnflushedrate":<Double_value>,

"tcperrcltretrasmitrate":<Double_value>,

"tcperrcookiepktmssreject":<Double_value>,

"tcperrretransmitgiveuprate":<Double_value>,

"tcperrsynsentbadack":<Double_value>,
```

```
"tcperrfastretransmissionsrate":<Double_value>,

"tcperrrstintimewait":<Double_value>,

"tcpcurclientconnestablished":<Double_value>,

"tcpcurclientconnopening":<Double_value>,

"tcpcurserverconnclosing":<Double_value>,

"tcperrretransmitrate":<Double_value>,

"tcperrsynretry":<Double_value>,

"tcperranyportfailrate":<Double_value>,

"tcperrrstnonestrate":<Double_value>,

"tcpzombieactivehalfclosecltconnflushedrate":<Double_value>,

"tcperrretransmit":<Double_value>,

"tcpsurgequeuelen":<Double_value>,

"tcperrcookiepktseqreject":<Double_value>,

"tcperrrstoutofwindowrate":<Double_value>,

"tcptotsynflush":<Double_value>,

"tcperrrstrate":<Double_value>,

"tcpcurserverconnopening":<Double_value>,

"tcperrsecondretransmissionsrate":<Double_value>,

"tcpcurclientconnclosing":<Double_value>,

"tcperrdataafterfinrate":<Double_value>,

"tcperrsyninestrate":<Double_value>,

"tcpsynproberate":<Double_value>,
```

```
"tcpsvrfinrate":<Double_value>,

"tcperrcipallocrate":<Double_value>,

"tcprxpktsrate":<Double_value>,

"tcperrbadchecksumrate":<Double_value>,

"tcperrrst":<Double_value>,

"tcperrrstthreshold":<Double_value>,

"tcperrsyngiveup":<Double_value>,

"tcperrrstintimewaitrate":<Double_value>,

"tcperrsynsentbadackrate":<Double_value>,

"tcpcurserverconn":<Double_value>,

"tcperrpartialretrasmit":<Double_value>,

"tcptotzombieactivehalfclosesvrconnflushed":<Double_value>,

"tcpserverconnopenedrate":<Double_value>,

"tcptottxbytes":<Double_value>,

"tcperrsyndroppedcongestionrate":<Double_value>,

"tcptotzombiecltconnflushed":<Double_value>,

"tcperrrstoutofwindow":<Double_value>,

"tcpwaittosyn":<Double_value>,

"tcperrbadstateconn":<Double_value>,

"tcprxbytesrate":<Double_value>,

"tcpsynrate":<Double_value>,

"tcptxbytesrate":<Double_value>,
```

```
"tcptotfinwaitclosed":<Double_value>,

"tcperrsyninsynrcvd":<Double_value>,

"tcperrfifthretransmissions":<Double_value>,

"tcptotzombiepassivehalfclosecltconnflushed":<Double_value>,

"tcperrsvrretrasmit":<Double_value>,

"tcperrbadchecksum":<Double_value>,

"tcperroutofwindowpktsrate":<Double_value>,

"tcperrcltoutoforder":<Double_value>,

"tcpzombiepassivehalfclosesrvconnflushedrate":<Double_value>,

"tcperranyportfail":<Double_value>,

"tcpfinwaitclosedrate":<Double_value>,

"tcpcurserverconnestablished":<Double_value>,

"tcptotserverconnopened":<Double_value>,

"tcperrsvrholerate":<Double_value>,

"tcperrsixthretransmissionsrate":<Double_value>,

"pcbzombiecallrate":<Double_value>,

"tcpzombiecltconnflushedrate":<Double_value>,

"tcpsynflushrate":<Double_value>,

"tcpwaittodata":<Double_value>,

"tcperrsynretryrate":<Double_value>,

"tcpwaittosynrate":<Double_value>,

"tcperrthirdretransmissionsrate":<Double_value>,
```

```
"tcptxpktsrate":<Double_value>,

"tcpzombiehalfopensvrconnflushedrate":<Double_value>,

"tcperrretransmitgiveup":<Double_value>,

"tcperrsvroutoforder":<Double_value>,

"tcperrcltholerate":<Double_value>,

"pcbtotzombiecall":<Double_value>,

"tcperrcookiepktseqdrop":<Double_value>,

"tcptotrxpkts":<Double_value>,

"tcperripportfailrate":<Double_value>,

"tcptotzombiepassivehalfclosesrvconnflushed":<Double_value>,

"tcperrfullretrasmitrate":<Double_value>,

"tcperrforthretransmissions":<Double_value>,

"tcptotsynheld":<Double_value>,

"tcperrsyninest":<Double_value>,

"tcpspareconn":<Double_value>,

"tcperrfingiveuprate":<Double_value>,

"tcperrcipalloc":<Double_value>,

"tcpclientconnopenedrate":<Double_value>,

"tcperrfastretransmissions":<Double_value>,

"tcperrsentrstrate":<Double_value>,

"tcperrcltretrasmit":<Double_value>,

"tcperripportfail":<Double_value>
```

```
}]}
```

protocoludp

Statistics for UDP Protocol resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full
udptotrxpkts	<Double>	Read-only	Total number of UDP packets received.
udprxpktsrate	<Double>	Read-only	Rate (/s) counter for udptotrxpkts
udptotrxbytes	<Double>	Read-only	Total number of UDP data received in bytes.
udprxbytesrate	<Double>	Read-only	Rate (/s) counter for udptotrxbytes
udptottxpkts	<Double>	Read-only	Total number of UDP packets transmitted.
udptxpktsrate	<Double>	Read-only	Rate (/s) counter for udptottxpkts
udptottxbytes	<Double>	Read-only	Total number of UDP data transmitted in bytes.
udptxbytesrate	<Double>	Read-only	Rate (/s) counter for udptottxbytes

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
udpcurratethreshold	<Double>	Read-only	Limit for UDP packets handled every 10 milliseconds. Default value, 0, applies no limit. This is a configurable value using the set rateControl command.
udptotunknownsvcpkts	<Double>	Read-only	Stray UDP packets dropped due to no configured listening service.
udpbadchecksum	<Double>	Read-only	Packets received with a UDP checksum error.
udpcurratethresholdexceeds	<Double>	Read-only	Number of times the UDP rate threshold is exceeded. If this counter continuously increases, first make sure the UDP packets received are genuine. If they are, increase the current rate threshold. This is a configurable value using the set rateControl command.

Operations

(click to see Properties)

- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/protocoludp **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/protocoludp? **args=detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get protocoludp resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/protocoludp? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "protocoludp": [ {

"udptotrxbytes":<Double_value>,

"udpcurratethresholdexceeds":<Double_value>,

"udptotunknownsvcpkts":<Double_value>,

"udptottxpkts":<Double_value>,

"udpcurratethreshold":<Double_value>,

"udptxbytesrate":<Double_value>,

"udptotrxpkts":<Double_value>,

"udpbadchecksum":<Double_value>,

"udptxpktsrate":<Double_value>,

"udprxpktsrate":<Double_value>,

"udprxbytesrate":<Double_value>,

"udptottxbytes":<Double_value>

}]}
```

qos

Qos

QoS statistics.

NAME	DESCRIPTION
qos	Statistics for qos.

qos

Statistics for qos.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	.
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full
snmpqosqos_packets_received	<Double>	Read-only	Receive direction packets processed by QoS
snmpqosqos_packets_receivedrate	<Double>	Read-only	Rate (/s) counter for snmpqosqos_packets_received
snmpqosqos_packets_sent	<Double>	Read-only	Send direction packets processed by QoS
snmpqosqos_packets_sentrate	<Double>	Read-only	Rate (/s) counter for snmpqosqos_packets_sent

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
snmpqosqos_packets_bypassed	<Double>	Read-only	Packets bypassing QoS
snmpqosqos_packets_bypassedrate	<Double>	Read-only	Rate (/s) counter for snmpqosqos_packets_bypassed
snmpqosqos_packets_dropped	<Double>	Read-only	Total packets dropped
snmpqosqos_packets_droppedrate	<Double>	Read-only	Rate (/s) counter for snmpqosqos_packets_dropped
snmpqosqos_bytes_rx	<Double>	Read-only	Received bytes processed by QoS
snmpqosqos_bytes_rxrate	<Double>	Read-only	Rate (/s) counter for snmpqosqos_bytes_rx
snmpqosqos_bytes_tx	<Double>	Read-only	Sent bytes processed by QoS
snmpqosqos_bytes_txrate	<Double>	Read-only	Rate (/s) counter for snmpqosqos_bytes_tx
snmpqosqos_lazy_bytes	<Double>	Read-only	QoS lazy byte optimization rate
snmpqosqos_lazy_bytesrate	<Double>	Read-only	Rate (/s) counter for snmpqosqos_lazy_bytes
snmpqosqos_real_bytes	<Double>	Read-only	QoS actual bytes scheduled
snmpqosqos_real_bytesrate	<Double>	Read-only	Rate (/s) counter for snmpqosqos_real_bytes

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
snmpqosqos_packets_filtered	<Double>	Read-only	Total packets filtered by QoS
snmpqosqos_packets_filteredrate	<Double>	Read-only	Rate (/s) counter for snmpqosqos_packets_filtered
snmpqosqos_packets_classified	<Double>	Read-only	Total packets classified by QoS
snmpqosqos_packets_classifiedrate	<Double>	Read-only	Rate (/s) counter for snmpqosqos_packets_classified
snmpqosqos_flows	<Double>	Read-only	New QoS flows
snmpqosqos_flowsrate	<Double>	Read-only	Rate (/s) counter for snmpqosqos_flows
snmpqosqos_flow_recycles	<Double>	Read-only	Recycled QoS flows
snmpqosqos_flow_recyclesrate	<Double>	Read-only	Rate (/s) counter for snmpqosqos_flow_recycles
snmpqosqos_session_recycle_failure	<Double>	Read-only	QoS Flow Recycle failures
snmpqosqos_session_recycle_failurerate	<Double>	Read-only	Rate (/s) counter for snmpqosqos_session_recycle_failure
snmpqosqos_sessions_ignored	<Double>	Read-only	Sessions manually ignored
snmpqosqos_sessions_ignoredrate	<Double>	Read-only	Rate (/s) counter for snmpqosqos_sessions_ignored

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
snmpqosqos_sessions_consumed	<Double>	Read-only	sessions manually consumed
snmpqosqos_sessions_consumedrate	<Double>	Read-only	Rate (/s) counter for snmpqosqos_sessions_consumed
snmpqosqos_actions_created	<Double>	Read-only	Uneque qos action objects created
snmpqosqos_actions_createdrate	<Double>	Read-only	Rate (/s) counter for snmpqosqos_actions_created
snmpqosqos_policy_reeval	<Double>	Read-only	Policies re-evaluated due to cli change
snmpqosqos_policy_reevalrate	<Double>	Read-only	Rate (/s) counter for snmpqosqos_policy_reeval
snmpqosqos_cfy_tcp_unknown	<Double>	Read-only	Connections unable to be classified beyond TCP
snmpqosqos_cfy_tcp_unknownrate	<Double>	Read-only	Rate (/s) counter for snmpqosqos_cfy_tcp_unknown
snmpqosqos_cfy_udp_unknown	<Double>	Read-only	Connections unable to be classified beyond UDP
snmpqosqos_cfy_udp_unknownrate	<Double>	Read-only	Rate (/s) counter for snmpqosqos_cfy_udp_unknown
snmpqosqos_sch_leafs	<Double>	Read-only	Scheduler leaf nodes constructed

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
snmpqosqos_sch_leafsrate	<Double>	Read-only	Rate (/s) counter for snmpqosqos_sch_leafs
snmpqosqos_session_mem	<Double>	Read-only	Session memory allocated
snmpqosqos_session_memrate	<Double>	Read-only	Rate (/s) counter for snmpqosqos_session_mem
snmpqosqos_sch_virtual_packets	<Double>	Read-only	Scheduler virtual packets constructed
snmpqosqos_sch_virtual_packetsrate	<Double>	Read-only	Rate (/s) counter for snmpqosqos_sch_virtual_packets
snmpqosqos_sch_virtual_bytes_accepted	<Double>	Read-only	Scheduler bytes accepted
snmpqosqos_sch_virtual_bytes_acceptedrate	<Double>	Read-only	Rate (/s) counter for snmpqosqos_sch_virtual_bytes_accepted
snmpqosqos_sch_leaf_recycle_failures	<Double>	Read-only	Scheduler Failures to recycle QoS flows
snmpqosqos_sch_leaf_recycle_failuresrate	<Double>	Read-only	Rate (/s) counter for snmpqosqos_sch_leaf_recycle_failures
snmpqosqos_sch_node_regulated_count	<Double>	Read-only	Scheduler Regulated node count
snmpqosqos_sch_node_regulated_countrate	<Double>	Read-only	Rate (/s) counter for snmpqosqos_sch_node_regulated_count
snmpqosqos_sch_sessions_created	<Double>	Read-only	Scheduler session classes constructed

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
snmpqosqos_sch_sessions_createdrate	<Double>	Read-only	Rate (/s) counter for snmpqosqos_sch_sessions_created
snmpqosqos_sch_sessions_deleted	<Double>	Read-only	Scheduler session classes constructed
snmpqosqos_sch_sessions_deletedrate	<Double>	Read-only	Rate (/s) counter for snmpqosqos_sch_sessions_deleted
snmpqosqos_sch_sdrr_nodes	<Double>	Read-only	Scheduler sdrr nodes constructed
snmpqosqos_sch_sdrr_nodesrate	<Double>	Read-only	Rate (/s) counter for snmpqosqos_sch_sdrr_nodes
snmpqosqos_sch_session_conns	<Double>	Read-only	Scheduler session connections created
snmpqosqos_sch_session_connsrate	<Double>	Read-only	Rate (/s) counter for snmpqosqos_sch_session_conns
snmpqosqos_sch_session_conns_removed	<Double>	Read-only	Scheduler session connections removed
snmpqosqos_sch_session_conns_removedrate	<Double>	Read-only	Rate (/s) counter for snmpqosqos_sch_session_conns_removed
snmpqosqos_sch_sessions_regulated_count	<Double>	Read-only	Scheduler regulated sessions count
snmpqosqos_sch_sessions_regulated_countrate	<Double>	Read-only	Rate (/s) counter for snmpqosqos_sch_se

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			ssions_regulated_count
snmpqosqos_sch_sessions_byte_count	<Double>	Read-only	Scheduler session bytes total
snmpqosqos_sch_sessions_byte_countrate	<Double>	Read-only	Rate (/s) counter for snmpqosqos_sch_sessions_byte_count
snmpqosqos_sch_regulated_count	<Double>	Read-only	Scheduler regulated node count
snmpqosqos_sch_regulated_countrate	<Double>	Read-only	Rate (/s) counter for snmpqosqos_sch_regulated_count
snmpqosqos_sch_links_created	<Double>	Read-only	Scheduler links created
snmpqosqos_sch_links_createdrate	<Double>	Read-only	Rate (/s) counter for snmpqosqos_sch_links_created
snmpqosqos_sch_links_deleted	<Double>	Read-only	Scheduler links deleted
snmpqosqos_sch_links_deletedrate	<Double>	Read-only	Rate (/s) counter for snmpqosqos_sch_links_deleted
snmpqosqos_sch_links_updated	<Double>	Read-only	Scheduler links updated
snmpqosqos_sch_links_updatedrate	<Double>	Read-only	Rate (/s) counter for snmpqosqos_sch_links_updated
snmpqosqos_sch_poll_count	<Double>	Read-only	Scheduler calls to poll_libqos

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
snmpqosqos_sch_poll_countrate	<Double>	Read-only	Rate (/s) counter for snmpqosqos_sch_poll_count
snmpqosqos_sch_peer_msgs	<Double>	Read-only	Scheduler peer messages received
snmpqosqos_sch_peer_msgsrate	<Double>	Read-only	Rate (/s) counter for snmpqosqos_sch_peer_msgs
snmpqosqos_error_ipc	<Double>	Read-only	IPC failed for QoS messages.
snmpqosqos_error_ipcrate	<Double>	Read-only	Rate (/s) counter for snmpqosqos_error_ipc
snmpqosqos_flow_mem	<Double>	Read-only	Flow memory allocated
snmpqosqos_flow_memrate	<Double>	Read-only	Rate (/s) counter for snmpqosqos_flow_mem
snmpqosqos_flows_available	<Double>	Read-only	Flows free list size
snmpqosqos_flows_availablerate	<Double>	Read-only	Rate (/s) counter for snmpqosqos_flows_available
snmpqosqos_recycle_failed_backlog	<Double>	Read-only	Recycle failed due to backlog
snmpqosqos_recycle_failed_backlograte	<Double>	Read-only	Rate (/s) counter for snmpqosqos_recycle_failed_backlog
snmpqosqos_recycle_failed_session	<Double>	Read-only	Recycle failed due to session attachment

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
snmpqosqos_recycle_failed_sessionrate	<Double>	Read-only	Rate (/s) counter for snmpqosqos_recycle_failed_session
snmpqosqos_error_create_action_failed	<Double>	Read-only	Failed attempts to create actions
snmpqosqos_error_create_action_failedrate	<Double>	Read-only	Rate (/s) counter for snmpqosqos_error_create_action_failed
snmpqosqos_error_modify_action_failed	<Double>	Read-only	Failed attempts to modify actions
snmpqosqos_error_modify_action_failedrate	<Double>	Read-only	Rate (/s) counter for snmpqosqos_error_modify_action_failed
snmpqosqos_error_remove_action_failed	<Double>	Read-only	Failed attempts to remove actions
snmpqosqos_error_remove_action_failedrate	<Double>	Read-only	Rate (/s) counter for snmpqosqos_error_remove_action_failed
snmpqosqos_error_cli_unknown	<Double>	Read-only	Internal CLI error
snmpqosqos_error_cli_unknownrate	<Double>	Read-only	Rate (/s) counter for snmpqosqos_error_cli_unknown
snmpqosqos_error_rename_not_implemented	<Double>	Read-only	qos action rename not yet implemented
snmpqosqos_error_rename_not_implementedrate	<Double>	Read-only	Rate (/s) counter for snmpqosqos_error_rename_not_implemented

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
snmpqosqos_error_remove_policy_failed	<Double>	Read-only	Failed attempts to remove qos policy
snmpqosqos_error_remove_policy_failedrate	<Double>	Read-only	Rate (/s) counter for snmpqosqos_error_remove_policy_failed
snmpqosqos_error_create_policy_failed	<Double>	Read-only	Failed attempts to create qos policy
snmpqosqos_error_create_policy_failedrate	<Double>	Read-only	Rate (/s) counter for snmpqosqos_error_create_policy_failed
snmpqosqos_error_libqos_api_failures	<Double>	Read-only	Libqos api failures
snmpqosqos_error_libqos_api_failuresrate	<Double>	Read-only	Rate (/s) counter for snmpqosqos_error_libqos_api_failures
snmpqosqos_error_api_ses_invalidpcb	<Double>	Read-only	Libqos api qos_session_add_pcb/natpcb() failed for reason QS_EINVALIDPCB
snmpqosqos_error_api_ses_invalidpcbrate	<Double>	Read-only	Rate (/s) counter for snmpqosqos_error_api_ses_invalidpcb
snmpqosqos_error_api_ses_notready	<Double>	Read-only	Libqos api qos_session_add_pcb/natpcb() failed for reason QS_ENOTREADY
snmpqosqos_error_api_ses_notreadyrate	<Double>	Read-only	Rate (/s) counter for snmpqosqos_error_api_ses_notready

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
snmpqosqos_error_api_ses_add_insession	<Double>	Read-only	Libqos api qos_session_add_pcb/natpcb() failed for reason QS_EINSESSION
snmpqosqos_error_api_ses_add_insessionrate	<Double>	Read-only	Rate (/s) counter for snmpqosqos_error_api_ses_add_insession
snmpqosqos_error_api_ses_add_other	<Double>	Read-only	Libqos api qos_session_add_pcb/natpcb() failed
snmpqosqos_error_api_ses_add_otherrate	<Double>	Read-only	Rate (/s) counter for snmpqosqos_error_api_ses_add_other
snmpqosqos_error_api_ses_rem_notinsession	<Double>	Read-only	Libqos api qos_session_rem_pcb/natpcb() failed for reason QS_ENOTINSESSION
snmpqosqos_error_api_ses_rem_notinsessionrate	<Double>	Read-only	Rate (/s) counter for snmpqosqos_error_api_ses_rem_notinsession
snmpqosqos_error_api_ses_rem_other	<Double>	Read-only	Libqos api qos_session_rem_pcb/natpcb() failed
snmpqosqos_error_api_ses_rem_otherrate	<Double>	Read-only	Rate (/s) counter for snmpqosqos_error_api_ses_rem_other

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
snmpqosqos_error_api_ses_del	<Double>	Read-only	Libqos api qos_session_delete faled
snmpqosqos_error_api_ses_delrate	<Double>	Read-only	Rate (/s) counter for snmpqosqos_error_api_ses_del
snmpqosqos_error_no_flows	<Double>	Read-only	Libqos out of flow memory
snmpqosqos_error_no_flowsrate	<Double>	Read-only	Rate (/s) counter for snmpqosqos_error_no_flows
snmpqosqos_error_no_sessions	<Double>	Read-only	Libqos out of session memory
snmpqosqos_error_no_sessionsrate	<Double>	Read-only	Rate (/s) counter for snmpqosqos_error_no_sessions

Operations

(click to see Properties)

- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of

creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/qos **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/qos? **args=name: <String_value> ,detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get qos resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/qos? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "qos": [ {

"snmpqosqos_error_remove_policy_failedrate":<Double_value>,

"snmpqosqos_cfy_udp_unknown":<Double_value>,

"snmpqosqos_sch_sessions_deletedrate":<Double_value>,

"snmpqosqos_sch_leafsrate":<Double_value>,

"snmpqosqos_flow_mem":<Double_value>,

"snmpqosqos_sch_virtual_packetsrate":<Double_value>,

"snmpqosqos_error_api_ses_add_insessionrate":<Double_value>,

"snmpqosqos_sch_leaf_recycle_failuresrate":<Double_value>,

"snmpqosqos_sch_sessions_regulated_count":<Double_value>,

"snmpqosqos_bytes_txrate":<Double_value>,

"snmpqosqos_sch_leaf_recycle_failures":<Double_value>,

"snmpqosqos_sch_poll_countrate":<Double_value>,

"snmpqosqos_error_api_ses_rem_otherrate":<Double_value>,

"snmpqosqos_error_create_action_failedrate":<Double_value>,

"snmpqosqos_error_rename_not_implementedrate":<Double_value>,

"snmpqosqos_packets_filtered":<Double_value>,

"snmpqosqos_error_ipc":<Double_value>,

"snmpqosqos_sch_sdrr_nodesrate":<Double_value>,

"snmpqosqos_recycle_failed_session":<Double_value>,

"snmpqosqos_sch_links_deleted":<Double_value>,

"snmpqosqos_error_remove_action_failed":<Double_value>,
```

```
"snmpqosqos_sch_sessions_createdrate":<Double_value>,

"snmpqosqos_flows_availablerate":<Double_value>,

"snmpqosqos_cfy_udp_unknownrate":<Double_value>,

"snmpqosqos_error_ipcrate":<Double_value>,

"snmpqosqos_sch_sdrr_nodes":<Double_value>,

"snmpqosqos_policy_reevalrate":<Double_value>,

"snmpqosqos_sch_peer_msgs":<Double_value>,

"snmpqosqos_error_api_ses_notready":<Double_value>,

"snmpqosqos_error_remove_policy_failed":<Double_value>,

"snmpqosqos_packets_droppedrate":<Double_value>,

"snmpqosqos_flows_available":<Double_value>,

"snmpqosqos_sch_leafs":<Double_value>,

"snmpqosqos_sessions_ignoredrate":<Double_value>,

"snmpqosqos_sch_node_regulated_countrate":<Double_value>,

"snmpqosqos_recycle_failed_backlograte":<Double_value>,

"snmpqosqos_sch_virtual_bytes_accepted":<Double_value>,

"snmpqosqos_flow_recyclesrate":<Double_value>,

"snmpqosqos_error_cli_unknownrate":<Double_value>,

"snmpqosqos_packets_sent":<Double_value>,

"snmpqosqos_sch_virtual_bytes_acceptedrate":<Double_value>,

"snmpqosqos_error_api_ses_rem_other":<Double_value>,

"snmpqosqos_sch_links_createdrate":<Double_value>,
```

```
"snmpqosqos_sch_session_conns_removedrate":<Double_value>,

"snmpqosqos_error_create_policy_failedrate":<Double_value>,

"snmpqosqos_error_api_ses_add_other":<Double_value>,

"snmpqosqos_packets_receivedrate":<Double_value>,

"snmpqosqos_sch_node_regulated_count":<Double_value>,

"snmpqosqos_packets_sentrate":<Double_value>,

"snmpqosqos_error_create_action_failed":<Double_value>,

"snmpqosqos_sch_links_created":<Double_value>,

"snmpqosqos_sch_links_updated":<Double_value>,

"snmpqosqos_sch_virtual_packets":<Double_value>,

"snmpqosqos_sch_sessions_deleted":<Double_value>,

"snmpqosqos_error_no_sessions":<Double_value>,

"snmpqosqos_session_mem":<Double_value>,

"snmpqosqos_policy_reeval":<Double_value>,

"snmpqosqos_sch_poll_count":<Double_value>,

"snmpqosqos_error_libqos_api_failures":<Double_value>,

"snmpqosqos_session_recycle_failurerate":<Double_value>,

"snmpqosqos_error_create_policy_failed":<Double_value>,

"snmpqosqos_sch_session_conns":<Double_value>,

"snmpqosqos_packets_classifiedrate":<Double_value>,

"snmpqosqos_error_api_ses_rem_notinsession":<Double_value>,

"snmpqosqos_bytes_rx":<Double_value>,
```

```
"snmpqosqos_packets_classified":<Double_value>,

"snmpqosqos_error_modify_action_failed":<Double_value>,

"snmpqosqos_recycle_failed_sessionrate":<Double_value>,

"snmpqosqos_packets_dropped":<Double_value>,

"snmpqosqos_sch_session_connsrate":<Double_value>,

"snmpqosqos_actions_createdrate":<Double_value>,

"snmpqosqos_error_remove_action_failedrate":<Double_value>,

"snmpqosqos_session_memrate":<Double_value>,

"snmpqosqos_error_api_ses_delrate":<Double_value>,

"snmpqosqos_sch_sessions_byte_countrate":<Double_value>,

"snmpqosqos_error_modify_action_failedrate":<Double_value>,

"snmpqosqos_error_api_ses_rem_notinsessionrate":<Double_value>,

"snmpqosqos_cfy_tcp_unknownrate":<Double_value>,

"snmpqosqos_session_recycle_failure":<Double_value>,

"snmpqosqos_packets_bypassed":<Double_value>,

"snmpqosqos_bytes_rxrate":<Double_value>,

"snmpqosqos_packets_bypassedrate":<Double_value>,

"snmpqosqos_sessions_ignored":<Double_value>,

"snmpqosqos_sch_regulated_countrate":<Double_value>,

"snmpqosqos_flow_recycles":<Double_value>,

"snmpqosqos_error_api_ses_del":<Double_value>,

"snmpqosqos_error_libqos_api_failuresrate":<Double_value>,
```

```
"snmpqosqos_lazy_bytesrate":<Double_value>,

"snmpqosqos_flows":<Double_value>,

"snmpqosqos_error_no_flows":<Double_value>,

"snmpqosqos_flowsrate":<Double_value>,

"snmpqosqos_actions_created":<Double_value>,

"snmpqosqos_sch_peer_msgsrate":<Double_value>,

"snmpqosqos_error_api_ses_invalidpcbrate":<Double_value>,

"snmpqosqos_sch_sessions_regulated_countrate":<Double_value>,

"snmpqosqos_recycle_failed_backlog":<Double_value>,

"snmpqosqos_sch_sessions_byte_count":<Double_value>,

"snmpqosqos_error_rename_not_implemented":<Double_value>,

"snmpqosqos_bytes_tx":<Double_value>,

"snmpqosqos_error_api_ses_notreadyrate":<Double_value>,

"snmpqosqos_real_bytes":<Double_value>,

"snmpqosqos_sch_links_updatedrate":<Double_value>,

"snmpqosqos_flow_memrate":<Double_value>,

"snmpqosqos_sch_links_deletedrate":<Double_value>,

"snmpqosqos_sessions_consumed":<Double_value>,

"snmpqosqos_error_no_flowsrate":<Double_value>,

"snmpqosqos_error_api_ses_add_otherrate":<Double_value>,

"snmpqosqos_packets_received":<Double_value>,

"snmpqosqos_sessions_consumedrate":<Double_value>,
```

```
"snmpqosqos_packets_filteredrate":<Double_value>,

"snmpqosqos_error_cli_unknown":<Double_value>,

"snmpqosqos_error_api_ses_invalidpcb":<Double_value>,

"snmpqosqos_lazy_bytes":<Double_value>,

"snmpqosqos_error_api_ses_add_insession":<Double_value>,

"snmpqosqos_cfy_tcp_unknown":<Double_value>,

"snmpqosqos_sch_regulated_count":<Double_value>,

"snmpqosqos_sch_session_conns_removed":<Double_value>,

"snmpqosqos_real_bytesrate":<Double_value>,

"snmpqosqos_sch_sessions_created":<Double_value>,

"snmpqosqos_error_no_sessionsrate":<Double_value>

}]}
```

responder

Responder

Responder statistics.

NAME	DESCRIPTION
responderpolicy	Statistics for responder policy resource.
responderpolicylabel	Statistics for responder policy label resource.

responderpolicy

Statistics for responder policy resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the responder policy for which to show detailed statistics. Minimum length = 1
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full
pipolicyhits	<Double>	Read-only	Number of hits on the policy
pipolicyhitsrate	<Double>	Read-only	Rate (/s) counter for pipolicyhits
pipolicyundefhits	<Double>	Read-only	Number of undef hits on the policy
pipolicyundefhitsrate	<Double>	Read-only	Rate (/s) counter for pipolicyundefhits

Operations

(click to see Properties)

- GET (ALL)
- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/responderpolicy **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/responderpolicy? **args=name: <String_value> ,detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get responderpolicy resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/responderpolicy? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "responderpolicy": [ {

"name":<String_value>,

"pipolicyhits":<Double_value>,

"pipolicyundefhits":<Double_value>,

"pipolicyhitsrate":<Double_value>,

"pipolicyundefhitsrate":<Double_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/stat/responderpolicy/ name_value><String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "responderpolicy": [ {

"name":<String_value>,

"pipolicyhits":<Double_value>,

"pipolicyundefhits":<Double_value>,

"pipolicyhitsrate":<Double_value>,

"pipolicyundefhitsrate":<Double_value>

}]}
```

responderpolicylabel

Statistics for responder policy label resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
labelname	<String>	Read-write	Name of the responder policy label. Minimum length = 1
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full
pipolicylabelhits	<Double>	Read-only	Number of times policy label was invoked.
pipolicylabelhitsrate	<Double>	Read-only	Rate (/s) counter for pipolicylabelhits

Operations

(click to see Properties)

- GET (ALL)
- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/responderpolicylabel **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/responderpolicylabel? **args=labelname: <String_value> ,detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get responderpolicylabel resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/responderpolicylabel? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "responderpolicylabel": [ {

"labelname":<String_value>,

"pipolicylabelhits":<Double_value>,

"pipolicylabelhitsrate":<Double_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/stat/responderpolicylabel/ labelname_value><String>
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "responderpolicylabel": [ {

"labelname":<String_value>,

"pipolicylabelhits":<Double_value>,

"pipolicylabelhitsrate":<Double_value>

}]}
```

rewrite

Rewrite

Rewrite statistics.

NAME	DESCRIPTION
rewritepolicy	Statistics for rewrite policy resource.
rewritepolicylabel	Statistics for rewrite policy label resource.

rewritepolicy

Statistics for rewrite policy resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the rewrite policy. Minimum length = 1
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full
pipolicyhits	<Double>	Read-only	Number of hits on the policy
pipolicyhitsrate	<Double>	Read-only	Rate (/s) counter for pipolicyhits
pipolicyundefhits	<Double>	Read-only	Number of undef hits on the policy
pipolicyundefhitsrate	<Double>	Read-only	Rate (/s) counter for pipolicyundefhits

Operations

(click to see Properties)

- GET (ALL)
- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of

creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/rewritepolicy **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/rewritepolicy? **args=name: <String_value> ,detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get rewritepolicy resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/rewritepolicy? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "rewritepolicy": [ {

"name":<String_value>,

"pipolicyhitsrate":<Double_value>,

"pipolicyundefhitsrate":<Double_value>,

"pipolicyhits":<Double_value>,

"pipolicyundefhits":<Double_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/stat/rewritepolicy/ name_value><String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "rewritepolicy": [ {

"name":<String_value>,

"pipolicyhitsrate":<Double_value>,
```

```
"pipolicyundefhitsrate":<Double_value>,

"pipolicyhits":<Double_value>,

"pipolicyundefhits":<Double_value>

}]}
```

rewritepolicylabel

Statistics for rewrite policy label resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
labelname	<String>	Read-write	Name of the rewrite policy label. Minimum length = 1
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full
pipolicylabelhits	<Double>	Read-only	Number of times policy label was invoked.
pipolicylabelhitsrate	<Double>	Read-only	Rate (/s) counter for pipolicylabelhits

Operations

(click to see Properties)

- GET (ALL)
- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/rewritepolicylabel **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/rewritepolicylabel? **args=labelname: <String_value> ,detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get rewritepolicylabel resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/rewritepolicylabel? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "rewritepolicylabel": [ {

"labelname":<String_value>,

"pipolicylabelhits":<Double_value>,

"pipolicylabelhitsrate":<Double_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/stat/rewritepolicylabel/ labelname_value><String>
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "rewritepolicylabel": [ {

"labelname":<String_value>,

"pipolicylabelhits":<Double_value>,

"pipolicylabelhitsrate":<Double_value>

}]}
```

snmp

SNMP

SNMP(Simple Network Management Protocol) statistics.

NAME	DESCRIPTION
snmp	Statistics for snmp.

snmp

Statistics for snmp.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full
snmptotrxpkts	<Double>	Read-only	SNMP packets received.
snmprxpktsrate	<Double>	Read-only	Rate (/s) counter for snmptotrxpkts

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
snmptottxpkts	<Double>	Read-only	SNMP packets transmitted.
snmptxpktsrate	<Double>	Read-only	Rate (/s) counter for snmptottxpkts
snmptotgetreqs	<Double>	Read-only	SNMP Get-Request PDUs that have been accepted and processed.
snmpgetreqsrate	<Double>	Read-only	Rate (/s) counter for snmptotgetreqs
snmptotgetnextreqs	<Double>	Read-only	SNMP Get-Next PDUs that have been accepted and processed.
snmpgetnextreqsrate	<Double>	Read-only	Rate (/s) counter for snmptotgetnextreqs
snmptotgetbulkreqs	<Double>	Read-only	SNMP Get-Bulk PDUs that have been accepted and processed.
snmpgetbulkreqsrate	<Double>	Read-only	Rate (/s) counter for snmptotgetbulkreqs
snmptotresponses	<Double>	Read-only	SNMP Get-Response PDUs that have been generated by the Citrix ADC.
snmpresponsesrate	<Double>	Read-only	Rate (/s) counter for snmptotresponses
snmptottraps	<Double>	Read-only	SNMP Trap PDUs that have been

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			generated by the Citrix ADC.
snmptoterrreqdropped	<Double>	Read-only	SNMP requests dropped.
snmptotparseerrs	<Double>	Read-only	Number of ASN.1 or BER errors encountered when decoding received SNMP Messages.
snmptotbadversions	<Double>	Read-only	Number of SNMP messages received, which were for an unsupported SNMP version.
snmptotbadcommname	<Double>	Read-only	SNMP messages received, which used an SNMP community name not known to the Citrix ADC.
snmptotbadcommuse	<Double>	Read-only	The total number of SNMP Messages received that represented an SNMP operation which was not allowed by the SNMP community named in the Message.
snmpunsupportedsecuritylevel	<Double>	Read-only	SNMP packets that were dropped because they requested a security level that was unknown to the Citrix

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			ADC or otherwise unavailable.
snmpnotintimewindow	<Double>	Read-only	SNMP packets that were dropped because they appeared outside of the authoritative SNMP engine's window.
snmpunknownusername	<Double>	Read-only	SNMP packets that were dropped because they referenced a user that was not known to the SNMP engine.
snmpunknownengineids	<Double>	Read-only	SNMP packets that were dropped because they referenced an SNMP engine ID that was not known to the Citrix ADC.
snmpwrongdigests	<Double>	Read-only	SNMP packets that were dropped because they did not contain the expected digest value.
snmpdecryptionerrors	<Double>	Read-only	SNMP packets that were dropped because they could not be decrypted.

Operations

(click to see Properties)

- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/snmp **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/snmp? **args=detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get snmp resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/snmp? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "snmp": [ {

"snmptotgetbulkreqs":<Double_value>,

"snmpdecryptionerrors":<Double_value>,

"snmptotparseerrs":<Double_value>,

"snmpnotintimewindow":<Double_value>,

"snmpwrongdigests":<Double_value>,

"snmptotgetnextreqs":<Double_value>,

"snmptxpktsrate":<Double_value>,

"snmptoterrreqdropped":<Double_value>,

"snmptotbadcommuse":<Double_value>,

"snmptotbadcommname":<Double_value>,

"snmprxpktsrate":<Double_value>,

"snmpunknownengineids":<Double_value>,

"snmpgetbulkreqsrate":<Double_value>,

"snmptottxpkts":<Double_value>,
```

```
"snmpresponsesrate":<Double_value>,

"snmptotresponses":<Double_value>,

"snmpgetreqsrate":<Double_value>,

"snmpunsupportedsecuritylevel":<Double_value>,

"snmptotgetreqs":<Double_value>,

"snmptottraps":<Double_value>,

"snmptotbadversions":<Double_value>,

"snmptotrxpkts":<Double_value>,

"snmpgetnextreqsrate":<Double_value>,

"snmpunknownusername":<Double_value>

}]}
```

spillover

Spillover

Spillover policies and actions.

NAME	DESCRIPTION
spilloverpolicy	Statistics for Spillover policy resource.

spilloverpolicy

Statistics for Spillover policy resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the spillover policy for which to show detailed statistics. Minimum length = 1
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full
pipolicyhits	<Double>	Read-only	Number of hits on the policy
pipolicyhitsrate	<Double>	Read-only	Rate (/s) counter for pipolicyhits
pipolicyundefhits	<Double>	Read-only	Number of undef hits on the policy
pipolicyundefhitsrate	<Double>	Read-only	Rate (/s) counter for pipolicyundefhits

Operations

(click to see Properties)

- GET (ALL)
- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/spilloverpolicy **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/spilloverpolicy? **args=name: <String_value> ,detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get spilloverpolicy resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/spilloverpolicy? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "spilloverpolicy": [ {

"name":<String_value>,

"pipolicyundefhitsrate":<Double_value>,

"pipolicyhitsrate":<Double_value>,

"pipolicyundefhits":<Double_value>,

"pipolicyhits":<Double_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/stat/spilloverpolicy/ name_value><String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "spilloverpolicy": [ {

"name":<String_value>,
```

```
"pipolicyundefhitsrate":<Double_value>,

"pipolicyhitsrate":<Double_value>,

"pipolicyundefhits":<Double_value>,

"pipolicyhits":<Double_value>

}]}
```

ssl

SSL

SSL statistics

NAME	DESCRIPTION
ssl	Statistics for ssl.
sslvserver	Statistics for SSL virtual server resource.

ssl

Statistics for ssl.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full
ssltothwdecbesecondary	<Double>	Read-only	Number of bytes decrypted on the back-end in

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			hardware on secondary card.
sslhwdecbesecondaryrate	<Double>	Read-only	Rate (/s) counter for ssltothwdecbesecondary
ssltothwdecfesecondary	<Double>	Read-only	Number of bytes decrypted on the front-end in hardware on secondary card.
sslhwdecfesecondaryrate	<Double>	Read-only	Rate (/s) counter for ssltothwdecfesecondary
ssltothwencbesecondary	<Double>	Read-only	Number of bytes encrypted on the back-end in hardware on secondary card.
sslhwencbesecondaryrate	<Double>	Read-only	Rate (/s) counter for ssltothwencbesecondary
ssltothwencfesecondary	<Double>	Read-only	Number of bytes encrypted on the front-end in hardware on secondary card.
sslhwencfesecondaryrate	<Double>	Read-only	Rate (/s) counter for ssltothwencfesecondary
sslecdsap521cryptoutilizationstat	<Double>	Read-only	Utilization of the hardware asymmetric crypto resource. Only valid values are 0-100%.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Only works on platforms with Intel crypto chips.
sslecdsap384cryptoutilizationstat	<Double>	Read-only	Utilization of the hardware asymmetric crypto resource. Only valid values are 0-100%. Only works on platforms with Intel crypto chips.
sslecdsap256cryptoutilizationstat	<Double>	Read-only	Utilization of the hardware asymmetric crypto resource. Only valid values are 0-100%. Only works on platforms with Intel crypto chips.
sslecdsap224cryptoutilizationstat	<Double>	Read-only	Utilization of the hardware asymmetric crypto resource. Only valid values are 0-100%. Only works on platforms with Intel crypto chips.
sslasymecdsacryptoutilizationstat	<Double>	Read-only	Utilization of the hardware asymmetric crypto resource. Only valid values are 0-100%. Only works on platforms with Intel crypto chips.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
sslecdhx25519cryptoutilizationstat	<Double>	Read-only	Utilization of the hardware asymmetric crypto resource. Only valid values are 0-100%. Only works on platforms with Intel crypto chips.
sslecdhp521cryptoutilizationstat	<Double>	Read-only	Utilization of the hardware asymmetric crypto resource. Only valid values are 0-100%. Only works on platforms with Intel crypto chips.
sslecdhp384cryptoutilizationstat	<Double>	Read-only	Utilization of the hardware asymmetric crypto resource. Only valid values are 0-100%. Only works on platforms with Intel crypto chips.
sslecdhp256cryptoutilizationstat	<Double>	Read-only	Utilization of the hardware asymmetric crypto resource. Only valid values are 0-100%. Only works on platforms with Intel crypto chips.
sslecdhp224cryptoutilizationstat	<Double>	Read-only	Utilization of the hardware asymmetric crypto resource. Only valid values are 0-100%.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Only works on platforms with Intel crypto chips.
sslasymecdhcryptoutilizationstat	<Double>	Read-only	Utilization of the hardware asymmetric crypto resource. Only valid values are 0-100%. Only works on platforms with Intel crypto chips.
sslasymdhcryptoutilizationstat	<Double>	Read-only	Utilization of the hardware asymmetric crypto resource. Only valid values are 0-100%. Only works on platforms with Intel crypto chips.
sslasymrsaotherscryptoutilizationstat	<Double>	Read-only	Utilization of the hardware asymmetric crypto resource. Only valid values are 0-100%. Only works on platforms with Intel crypto chips.
sslasymrsa1kcryptoutilizationstat	<Double>	Read-only	Utilization of the hardware asymmetric crypto resource. Only valid values are 0-100%. Only works on platforms with Intel crypto chips.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
sslasymrsa2kcryptoutilizationstat	<Double>	Read-only	Utilization of the hardware asymmetric crypto resource. Only valid values are 0-100%. Only works on platforms with Intel crypto chips.
sslasymrsa4kcryptoutilizationstat	<Double>	Read-only	Utilization of the hardware asymmetric crypto resource. Only valid values are 0-100%. Only works on platforms with Intel crypto chips.
sslasymrsacryptoutilizationstat	<Double>	Read-only	Utilization of the hardware asymmetric crypto resource. Only valid values are 0-100%. Only works on platforms with Intel crypto chips.
ssltotdechwsecondary	<Double>	Read-only	Number of bytes decrypted in hardware on secondary card.
ssldechwsecondaryrate	<Double>	Read-only	Rate (/s) counter for ssltotdechwsecondary
ssltotenchwsecondary	<Double>	Read-only	Number of bytes encrypted in hardware on secondary card.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
sslenchwsecondaryrate	<Double>	Read-only	Rate (/s) counter for ssltotenchwsecondary
sslsymcryptoutilizationstat	<Double>	Read-only	Utilization of the hardware symmetric crypto resource. Only valid values are 0-100%. Only works on platforms with Intel crypto chips.
sslasymcryptoutilizationstat	<Double>	Read-only	Utilization of the hardware asymmetric crypto resource. Only valid values are 0-100%. Only works on platforms with Intel crypto chips.
sslcryptoutilizationucs	<Double>	Read-only	Utilization of the hardware unaligned crypto resource. Only valid values are 0-100%. Only works on platforms with Intel QAT2.0 crypto chips.
sslcryptoutilizationath	<Double>	Read-only	Utilization of the hardware authentication crypto resource. Only valid values are 0-100%. Only works on platforms with Intel QAT2.0 crypto chips.
sslcryptoutilizationcph	<Double>	Read-only	Utilization of the hardware cipher

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			crypto resource. Only valid values are 0-100%. Only works on platforms with Intel QAT2.0 crypto chips.
sslcryptoutilizationsymm	<Double>	Read-only	Utilization of the hardware symmetric crypto resource. Only valid values are 0-100%. Only works on platforms with Intel QAT1 crypto chips.
sslcryptoutilizationasym	<Double>	Read-only	Utilization of the hardware asymmetric crypto resource. Only valid values are 0-100%. Only works on platforms with Intel crypto chips.
sslcryptoutilizationstat2nd	<Double>	Read-only	Utilization of the hardware crypto resource. Only valid values are 0-100%. Only works on N3FIPS+N3 hybrid platform.
sslcryptoutilizationstat	<Double>	Read-only	Utilization of the hardware crypto resource. Only valid values are 0-100%. Only works on platforms with Nitrox-3 chips.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
sslnumcardsupsecondary	<Double>	Read-only	Number of Add on SSL cards that are UP.
sslcardssecondary	<Double>	Read-only	Number of secondary SSL crypto cards present on the Citrix ADC.
sslcardstatus	<Double>	Read-only	Status of the SSL card(s). The value should be interpreted in binary form, with each set bit indicates a card as UP.
sslcards	<Double>	Read-only	Number of SSL crypto cards present on the Citrix ADC.
sslnumcardsup	<Double>	Read-only	Number of SSL cards that are UP. If the number of cards UP is lower than a threshold, a failover is initiated.
sslenginestatus	<Double>	Read-only	State of the SSL Engine (1=UP/ 0=DOWN). This state is decided based on SSL Feature/License status and minimum number of cards UP.
ssltotsessions	<Double>	Read-only	Number of SSL sessions on the Citrix ADC.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
sslsessionsrate	<Double>	Read-only	Rate (/s) counter for ssltotsessions
ssltottransactions	<Double>	Read-only	Number of SSL transactions on the Citrix ADC
ssltransactionsrate	<Double>	Read-only	Rate (/s) counter for ssltottransactions
ssltotsslv3transactions	<Double>	Read-only	Total number of SSLv3 transactions on the Citrix ADC.
sslsslv3transactionsrate	<Double>	Read-only	Rate (/s) counter for ssltotsslv3transactions
ssltottlsv1transactions	<Double>	Read-only	Number of TLSv1 transactions on the Citrix ADC.
ssltlsv1transactionsrate	<Double>	Read-only	Rate (/s) counter for ssltottlsv1transactions
ssltottlsv11transactions	<Double>	Read-only	Number of TLSv1.1 transactions on the Citrix ADC.
ssltlsv11transactionsrate	<Double>	Read-only	Rate (/s) counter for ssltottlsv11transactions
ssltottlsv12transactions	<Double>	Read-only	Number of TLSv1.2 transactions on the Citrix ADC.
ssltlsv12transactionsrate	<Double>	Read-only	Rate (/s) counter for ssltottlsv12transactions

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ssltottlsv13transactions	<Double>	Read-only	Number of TLSv1.3 transactions on the Citrix ADC.
ssltlsv13transactionsrate	<Double>	Read-only	Rate (/s) counter for ssltottlsv13transactions
ssltotdtlsv1transactions	<Double>	Read-only	Number of DTLSv1 transactions on the Citrix ADC.
ssldtlsv1transactionsrate	<Double>	Read-only	Rate (/s) counter for ssltotdtlsv1transactions
ssltotdtlsv12transactions	<Double>	Read-only	Number of DTLSv1.2 transactions on the Citrix ADC.
ssldtlsv12transactionsrate	<Double>	Read-only	Rate (/s) counter for ssltotdtlsv12transactions
ssltotsslv3sessions	<Double>	Read-only	Number of SSLv3 sessions on the Citrix ADC.
sslsslv3sessionsrate	<Double>	Read-only	Rate (/s) counter for ssltotsslv3sessions
ssltottlsv1sessions	<Double>	Read-only	Number of TLSv1 sessions on the Citrix ADC.
ssltlsv1sessionsrate	<Double>	Read-only	Rate (/s) counter for ssltottlsv1sessions
ssltottlsv11sessions	<Double>	Read-only	Number of TLSv1.1 sessions on the Citrix ADC.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ssltlsv11sessionsrate	<Double>	Read-only	Rate (/s) counter for ssltottlsv11sessions
ssltottlsv12sessions	<Double>	Read-only	Number of TLSv1.2 sessions on the Citrix ADC.
ssltlsv12sessionsrate	<Double>	Read-only	Rate (/s) counter for ssltottlsv12sessions
ssltottlsv13sessions	<Double>	Read-only	Number of TLSv1.3 sessions on the Citrix ADC.
ssltlsv13sessionsrate	<Double>	Read-only	Rate (/s) counter for ssltottlsv13sessions
ssltotdtlsv1sessions	<Double>	Read-only	Number of DTLSv1 sessions on the Citrix ADC.
ssldtlsv1sessionsrate	<Double>	Read-only	Rate (/s) counter for ssltotdtlsv1sessions
ssltotdtlsv12sessions	<Double>	Read-only	Number of DTLSv1.2 sessions on the Citrix ADC.
ssldtlsv12sessionsrate	<Double>	Read-only	Rate (/s) counter for ssltotdtlsv12sessions
ssltotnewsessions	<Double>	Read-only	Number of new SSL sessions created on the Citrix ADC.
sslnewsessionsrate	<Double>	Read-only	Rate (/s) counter for ssltotnewsessions
ssltotsessionmiss	<Double>	Read-only	Number of SSL session reuse

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			misses on the Citrix ADC.
sslsessionmissrate	<Double>	Read-only	Rate (/s) counter for ssltotsessionmiss
ssltotsessionhits	<Double>	Read-only	Number of SSL session reuse hits on the Citrix ADC.
sslsessionhitsrate	<Double>	Read-only	Rate (/s) counter for ssltotsessionhits
sslbetotsessions	<Double>	Read-only	Number of back-end SSL sessions on the Citrix ADC.
sslbesessionsrate	<Double>	Read-only	Rate (/s) counter for sslbetotsessions
sslbetotsslv3sessions	<Double>	Read-only	Number of back-end SSLv3 sessions on the Citrix ADC.
sslbesslv3sessionsrate	<Double>	Read-only	Rate (/s) counter for sslbetotsslv3sessions
sslbetottlsv1sessions	<Double>	Read-only	Number of back-end TLSv1 sessions on the Citrix ADC.
sslbetlsv1sessionsrate	<Double>	Read-only	Rate (/s) counter for sslbetottlsv1sessions
sslbetottlsv11sessions	<Double>	Read-only	Number of back-end TLSv1.1 sessions on the Citrix ADC.
sslbetlsv11sessionsrate	<Double>	Read-only	Rate (/s) counter for sslbetottlsv11sessions

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
sslbetottlsv12sessions	<Double>	Read-only	Number of back-end TLSv1.2 sessions on the Citrix ADC.
sslbetlsv12sessionsrate	<Double>	Read-only	Rate (/s) counter for sslbetottlsv12sessions
sslbetottlsv13sessions	<Double>	Read-only	Number of back-end TLSv1.3 sessions on the Citrix ADC.
sslbetlsv13sessionsrate	<Double>	Read-only	Rate (/s) counter for sslbetottlsv13sessions
sslbetotdtlsv1sessions	<Double>	Read-only	Number of back-end DTLSv1 sessions on the Citrix ADC.
sslbedtlsv1sessionsrate	<Double>	Read-only	Rate (/s) counter for sslbetotdtlsv1sessions
sslbetotdtlsv12sessions	<Double>	Read-only	Number of back-end DTLSv1.2 sessions on the Citrix ADC.
sslbedtlsv12sessionsrate	<Double>	Read-only	Rate (/s) counter for sslbetotdtlsv12sessions
sslbetotsessionmultiplexattempts	<Double>	Read-only	Number of back-end SSL session multiplex attempts on the Citrix ADC.
sslbesessionmultiplexattemptsrate	<Double>	Read-only	Rate (/s) counter for sslbetotsessionmultiplexattempts

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
sslbetotsessionmultiplexattemptsuccess	<Double>	Read-only	Number of back-end SSL session multiplex successes on the Citrix ADC.
sslbesessionmultiplexattemptsuccessrate	<Double>	Read-only	Rate (/s) counter for sslbetotsessionmultiplexattemptsuccess
sslbetotsessionmultiplexattemptfails	<Double>	Read-only	Number of back-end SSL session multiplex failures on the Citrix ADC.
sslbesessionmultiplexattemptfailsrate	<Double>	Read-only	Rate (/s) counter for sslbetotsessionmultiplexattemptfails
ssltotenc	<Double>	Read-only	Number of bytes encrypted on the Citrix ADC.
sslencrate	<Double>	Read-only	Rate (/s) counter for ssltotenc
ssltotdec	<Double>	Read-only	Number of bytes decrypted on the Citrix ADC.
ssldecrate	<Double>	Read-only	Rate (/s) counter for ssltotdec
ssltotsslserverinrecords	<Double>	Read-only	Number server in record on the Citrix ADC.
sslsslserverinrecordsrate	<Double>	Read-only	Rate (/s) counter for ssltotsslserverinrecords

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ssltotrenegsessions	<Double>	Read-only	Number of SSL session renegotiations on the Citrix ADC.
sslrenegsessionsrate	<Double>	Read-only	Rate (/s) counter for ssltotrenegsessions
ssltotsslv3renegsessions	<Double>	Read-only	Number of session renegotiations done on SSLv3.
sslsslv3renegsessionsrate	<Double>	Read-only	Rate (/s) counter for ssltotsslv3renegsessions
ssltottlsv1renegsessions	<Double>	Read-only	Number of SSL session renegotiations done on TLSv1.
ssltlsv1renegsessionsrate	<Double>	Read-only	Rate (/s) counter for ssltottlsv1renegsessions
ssltottlsv11renegsessions	<Double>	Read-only	Number of SSL session renegotiations done on TLSv1.1.
ssltlsv11renegsessionsrate	<Double>	Read-only	Rate (/s) counter for ssltottlsv11renegsessions
ssltottlsv12renegsessions	<Double>	Read-only	Number of SSL session renegotiations done on TLSv1.2.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ssltlsv12renegsessionsrate	<Double>	Read-only	Rate (/s) counter for ssltottlsv12renegsessions
ssltotdtlsv1renegsessions	<Double>	Read-only	Number of SSL session renegotiations done on DTLSv1.
ssldtlsv1renegsessionsrate	<Double>	Read-only	Rate (/s) counter for ssltotdtlsv1renegsessions
ssltotdtlsv12renegsessions	<Double>	Read-only	Number of SSL session renegotiations done on DTLSv1.2.
ssldtlsv12renegsessionsrate	<Double>	Read-only	Rate (/s) counter for ssltotdtlsv12renegsessions
ssltotrsa512keyexchanges	<Double>	Read-only	Number of RSA 512-bit key exchanges on the Citrix ADC.
sslrsa512keyexchangesrate	<Double>	Read-only	Rate (/s) counter for ssltotrsa512keyexchanges
ssltotrsa1024keyexchanges	<Double>	Read-only	Number of RSA 1024-bit key exchanges on the Citrix ADC.
sslrsa1024keyexchangesrate	<Double>	Read-only	Rate (/s) counter for ssltotrsa1024keyexchanges
ssltotrsa2048keyexchanges	<Double>	Read-only	Number of RSA 2048-bit key

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			exchanges on the Citrix ADC.
sslrsa2048keyexchangesrate	<Double>	Read-only	Rate (/s) counter for ssltotrsa2048keyexchanges
ssltotrsa3072keyexchanges	<Double>	Read-only	Number of RSA 3072-bit key exchanges on the Citrix ADC.
sslrsa3072keyexchangesrate	<Double>	Read-only	Rate (/s) counter for ssltotrsa3072keyexchanges
ssltotrsa4096keyexchanges	<Double>	Read-only	Number of RSA 4096-bit key exchanges on the Citrix ADC.
sslrsa4096keyexchangesrate	<Double>	Read-only	Rate (/s) counter for ssltotrsa4096keyexchanges
ssltotdh512keyexchanges	<Double>	Read-only	Number of Diffie-Helman 512-bit key exchanges on the Citrix ADC.
ssldh512keyexchangesrate	<Double>	Read-only	Rate (/s) counter for ssltotdh512keyexchanges
ssltotdh1024keyexchanges	<Double>	Read-only	Number of Diffie-Helman 1024-bit key exchanges on the Citrix ADC.
ssldh1024keyexchangesrate	<Double>	Read-only	Rate (/s) counter for ssltotdh1024keyexchanges

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ssltotdh2048keyexchanges	<Double>	Read-only	Number of Diffie-Helman 2048-bit key exchanges on the Citrix ADC.
ssldh2048keyexchangesrate	<Double>	Read-only	Rate (/s) counter for ssltotdh2048keyexchanges
ssltotdh3072keyexchanges	<Double>	Read-only	Number of Diffie-Helman 3072-bit key exchanges on the Citrix ADC.
ssldh3072keyexchangesrate	<Double>	Read-only	Rate (/s) counter for ssltotdh3072keyexchanges
ssltotdh4096keyexchanges	<Double>	Read-only	Number of Diffie-Helman 4096-bit key exchanges on the Citrix ADC.
ssldh4096keyexchangesrate	<Double>	Read-only	Rate (/s) counter for ssltotdh4096keyexchanges
ssltotpqcx25519mlkem768keyexchanges	<Double>	Read-only	Number of Post Quantum Crypto Key Exchanges Using X25519MLKEM768 Group on the Citrix ADC.
sslpqcx25519mlkem768keyexchangesrate	<Double>	Read-only	Rate (/s) counter for ssltotpqcx25519mlkem768keyexchanges
ssltotecdhe521keyexchanges	<Double>	Read-only	Number of 521 Elliptical Curve

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Diffie-Helman on the Citrix ADC.
sslecdhe521keyexchangesrate	<Double>	Read-only	Rate (/s) counter for ssltotecdhe521keyexchanges
ssltotecdhe384keyexchanges	<Double>	Read-only	Number of 384 Elliptical Curve Diffie-Helman on the Citrix ADC.
sslecdhe384keyexchangesrate	<Double>	Read-only	Rate (/s) counter for ssltotecdhe384keyexchanges
ssltotecdhe256keyexchanges	<Double>	Read-only	Number of 256 Elliptical Curve Diffie-Helman on the Citrix ADC.
sslecdhe256keyexchangesrate	<Double>	Read-only	Rate (/s) counter for ssltotecdhe256keyexchanges
ssltotecdhe224keyexchanges	<Double>	Read-only	Number of 224 Elliptical Curve Diffie-Helman on the Citrix ADC.
sslecdhe224keyexchangesrate	<Double>	Read-only	Rate (/s) counter for ssltotecdhe224keyexchanges
ssltotecdhe25519keyexchanges	<Double>	Read-only	Number of 25519 Elliptical Curve Diffie-Helman on the Citrix ADC.
sslecdhe25519keyexchangesrate	<Double>	Read-only	Rate (/s) counter for ssltotecdhe25519keyexchanges

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ssltotecdhetransactions	<Double>	Read-only	Total ECDHE Transactions on Citrix ADC.
sslecdhetransactionsrate	<Double>	Read-only	Rate (/s) counter for ssltotecdhetransactions
ssltot40bitrc4ciphers	<Double>	Read-only	Number of RC4 40-bit cipher encryptions on the Citrix ADC.
ssl40bitrc4ciphersrate	<Double>	Read-only	Rate (/s) counter for ssltot40bitrc4ciphers
ssltot56bitrc4ciphers	<Double>	Read-only	Number of RC4 56-bit cipher encryptions on the Citrix ADC.
ssl56bitrc4ciphersrate	<Double>	Read-only	Rate (/s) counter for ssltot56bitrc4ciphers
ssltot64bitrc4ciphers	<Double>	Read-only	Number of RC4 64-bit cipher encryptions on the Citrix ADC.
ssl64bitrc4ciphersrate	<Double>	Read-only	Rate (/s) counter for ssltot64bitrc4ciphers
ssltot128bitrc4ciphers	<Double>	Read-only	Number of RC4 128-bit cipher encryptions on the Citrix ADC.
ssl128bitrc4ciphersrate	<Double>	Read-only	Rate (/s) counter for ssltot128bitrc4ciphers
ssltot40bitdesciphers	<Double>	Read-only	Number of DES 40-bit cipher encryptions on the Citrix ADC.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ssl40bitdesciphersrate	<Double>	Read-only	Rate (/s) counter for ssltot40bitdesciphers
ssltot56bitdesciphers	<Double>	Read-only	Number of DES 56-bit cipher encryptions on the Citrix ADC.
ssl56bitdesciphersrate	<Double>	Read-only	Rate (/s) counter for ssltot56bitdesciphers
ssltot168bit3desciphers	<Double>	Read-only	Number of DES 168-bit cipher encryptions on the Citrix ADC.
ssl168bit3desciphersrate	<Double>	Read-only	Rate (/s) counter for ssltot168bit3desciphers
ssltotcipheraes128	<Double>	Read-only	Number of AES 128-bit cipher encryptions on the Citrix ADC.
sslcipheraes128rate	<Double>	Read-only	Rate (/s) counter for ssltotcipheraes128
ssltotcipheraes256	<Double>	Read-only	Number of AES 256-bit cipher encryptions on the Citrix ADC.
sslcipheraes256rate	<Double>	Read-only	Rate (/s) counter for ssltotcipheraes256
ssltot40bitrc2ciphers	<Double>	Read-only	Number of RC2 40-bit cipher encryptions on the Citrix ADC.
ssl40bitrc2ciphersrate	<Double>	Read-only	Rate (/s) counter for ssltot40bitrc2ciphers

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ssltot56bitrc2ciphers	<Double>	Read-only	Number of RC2 56-bit cipher encryptions on the Citrix ADC.
ssl56bitrc2ciphersrate	<Double>	Read-only	Rate (/s) counter for ssltot56bitrc2ciphers
ssltot128bitrc2ciphers	<Double>	Read-only	Number of RC2 128-bit cipher encryptions on the Citrix ADC.
ssl128bitrc2ciphersrate	<Double>	Read-only	Rate (/s) counter for ssltot128bitrc2ciphers
ssltot128bitaesgcmciphers	<Double>	Read-only	Number of AEC-GCM 128-bit cipher encryptions on the Citrix ADC.
ssl128bitaesgcmciphersrate	<Double>	Read-only	Rate (/s) counter for ssltot128bitaesgcmciphers
ssltot256bitaesgcmciphers	<Double>	Read-only	Number of AEC-GCM 256-bit cipher encryptions on the Citrix ADC.
ssl256bitaesgcmciphersrate	<Double>	Read-only	Rate (/s) counter for ssltot256bitaesgcmciphers
ssltotnullciphers	<Double>	Read-only	Number of Null cipher encryptions on the Citrix ADC.
sslnullciphersrate	<Double>	Read-only	Rate (/s) counter for ssltotnullciphers

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ssltotmd5mac	<Double>	Read-only	Number of MD5 hashes on the Citrix ADC.
sslmd5macrate	<Double>	Read-only	Rate (/s) counter for ssltotmd5mac
ssltotshamac	<Double>	Read-only	Number of SHA hashes on the Citrix ADC.
sslshamacrate	<Double>	Read-only	Rate (/s) counter for ssltotshamac
ssltotsha256mac	<Double>	Read-only	Number of SHA256 hashes on the Citrix ADC.
sslsha256macrate	<Double>	Read-only	Rate (/s) counter for ssltotsha256mac
ssltotsha384mac	<Double>	Read-only	Number of SHA384 hashes on the Citrix ADC.
sslsha384macrate	<Double>	Read-only	Rate (/s) counter for ssltotsha384mac
ssltotsslv3handshakes	<Double>	Read-only	Number of handshakes on SSLv3 on the Citrix ADC.
sslsslv3handshakesrate	<Double>	Read-only	Rate (/s) counter for ssltotsslv3handshakes
ssltottlsv1handshakes	<Double>	Read-only	Number of SSL handshakes on TLSv1 on the Citrix ADC.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ssltlsv1handshakesrate	<Double>	Read-only	Rate (/s) counter for ssltottlsv1handshakes
ssltottlsv11handshakes	<Double>	Read-only	Number of SSL handshakes on TLSv1.1 on the Citrix ADC.
ssltlsv11handshakesrate	<Double>	Read-only	Rate (/s) counter for ssltottlsv11handshakes
ssltottlsv12handshakes	<Double>	Read-only	Number of SSL handshakes on TLSv1.2 on the Citrix ADC.
ssltlsv12handshakesrate	<Double>	Read-only	Rate (/s) counter for ssltottlsv12handshakes
ssltottlsv13handshakes	<Double>	Read-only	Number of SSL handshakes on TLSv1.3 on the Citrix ADC.
ssltlsv13handshakesrate	<Double>	Read-only	Rate (/s) counter for ssltottlsv13handshakes
ssltotdtlsv1handshakes	<Double>	Read-only	Number of SSL handshakes on DTLSv1 on the Citrix ADC.
ssldtlsv1handshakesrate	<Double>	Read-only	Rate (/s) counter for ssltotdtlsv1handshakes

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ssltotdtlsv12handshakes	<Double>	Read-only	Number of SSL handshakes on DTLSv1.2 on the Citrix ADC.
ssldtlsv12handshakesrate	<Double>	Read-only	Rate (/s) counter for ssltotdtlsv12handshakes
ssltotsslv3clientauthentications	<Double>	Read-only	Number of client authentications done on SSLv3.
sslsslv3clientauthenticationsrate	<Double>	Read-only	Rate (/s) counter for ssltotsslv3clientauthentications
ssltottlsv1clientauthentications	<Double>	Read-only	Number of client authentications done on TLSv1.
ssltlsv1clientauthenticationsrate	<Double>	Read-only	Rate (/s) counter for ssltottlsv1clientauthentications
ssltottlsv11clientauthentications	<Double>	Read-only	Number of client authentications done on TLSv1.1.
ssltlsv11clientauthenticationsrate	<Double>	Read-only	Rate (/s) counter for ssltottlsv11clientauthentications
ssltottlsv12clientauthentications	<Double>	Read-only	Number of client authentications done on TLSv1.2.
ssltlsv12clientauthenticationsrate	<Double>	Read-only	Rate (/s) counter for ssltottlsv12clientauthentications

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ssltottlsv13clientauthentications	<Double>	Read-only	Number of client authentications done on TLSv1.3.
ssltlsv13clientauthenticationsrate	<Double>	Read-only	Rate (/s) counter for ssltottlsv13clientauthentications
ssltotdtlsv1clientauthentications	<Double>	Read-only	Number of client authentications done on DTLSv1.
ssldtlsv1clientauthenticationsrate	<Double>	Read-only	Rate (/s) counter for ssltotdtlsv1clientauthentications
ssltotdtlsv12clientauthentications	<Double>	Read-only	Number of client authentications done on DTLSv1.2.
ssldtlsv12clientauthenticationsrate	<Double>	Read-only	Rate (/s) counter for ssltotdtlsv12clientauthentications
ssltotrsaauthorizations	<Double>	Read-only	Number of RSA authentications on the Citrix ADC.
sslrsaauthorizationsrate	<Double>	Read-only	Rate (/s) counter for ssltotrsaauthorizations
ssltotdhauthorizations	<Double>	Read-only	Number of Diffie-Helman authentications on the Citrix ADC.
ssldhauthorizationsrate	<Double>	Read-only	Rate (/s) counter for ssltotdhauthorizations

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ssltotdssauthorizations	<Double>	Read-only	Total number of times DSS authorization is used on the Citrix ADC.
ssldssauthorizationsrate	<Double>	Read-only	Rate (/s) counter for ssltotdssauthorizations
ssltotecdsaauthorizations	<Double>	Read-only	Total number of times ECDSA authorization is used on the Citrix ADC.
sslecdsaauthorizationsrate	<Double>	Read-only	Rate (/s) counter for ssltotecdsaauthorizations
ssltotnullauthorizations	<Double>	Read-only	Number of Null authentications on the Citrix ADC.
sslnullauthorizationsrate	<Double>	Read-only	Rate (/s) counter for ssltotnullauthorizations
ssltotbkendsessionrenegotiate	<Double>	Read-only	Number of back-end SSL session renegotiations on the Citrix ADC.
sslbkendsessionrenegotiaterate	<Double>	Read-only	Rate (/s) counter for ssltotbkendsessionrenegotiate
ssltotbkendsslv3renego	<Double>	Read-only	Number of back-end SSLv3 session renegotiations on the Citrix ADC.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
sslbkendsslv3renegorate	<Double>	Read-only	Rate (/s) counter for ssltotbkendsslv3renego
ssltotbkendtlsvlrenego	<Double>	Read-only	Number of back-end TLSv1 session renegotiations on the Citrix ADC.
sslbkendtlsvlrenegorate	<Double>	Read-only	Rate (/s) counter for ssltotbkendtlsvlrenego
ssltotbkendtlsv11renego	<Double>	Read-only	Number of back-end TLSv1.1 session renegotiations on the Citrix ADC.
sslbkendtlsv11renegorate	<Double>	Read-only	Rate (/s) counter for ssltotbkendtlsv11renego
ssltotbkendtlsv12renego	<Double>	Read-only	Number of back-end TLSv1.2 session renegotiations on the Citrix ADC.
sslbkendtlsv12renegorate	<Double>	Read-only	Rate (/s) counter for ssltotbkendtlsv12renego
ssltotbkenddtlsvlrenego	<Double>	Read-only	Number of back-end DTLSv1 session renegotiations on the Citrix ADC.
sslbkenddtlsvlrenegorate	<Double>	Read-only	Rate (/s) counter for ssltotbkenddtlsvlrenego

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ssltotbkenddtlsvl2renego	<Double>	Read-only	Number of back-end DTLSv1.2 session renegotiations on the Citrix ADC.
sslbkenddtlsvl2renegorate	<Double>	Read-only	Rate (/s) counter for ssltotbkenddtlsvl2renego
sslbetotrsa512keyexchanges	<Double>	Read-only	Number of back-end RSA 512-bit key exchanges on the Citrix ADC.
sslbersa512keyexchangesrate	<Double>	Read-only	Rate (/s) counter for sslbetotrsa512keyexchanges
sslbetotrsa1024keyexchanges	<Double>	Read-only	Number of back-end RSA 1024-bit key exchanges on the Citrix ADC.
sslbersa1024keyexchangesrate	<Double>	Read-only	Rate (/s) counter for sslbetotrsa1024keyexchanges
sslbetotrsa2048keyexchanges	<Double>	Read-only	Number of back-end RSA 2048-bit key exchanges on the Citrix ADC.
sslbersa2048keyexchangesrate	<Double>	Read-only	Rate (/s) counter for sslbetotrsa2048keyexchanges
sslbetotrsa3072keyexchanges	<Double>	Read-only	Number of back-end RSA 3072-bit key exchanges on the Citrix ADC.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
sslbersa3072keyexchangesrate	<Double>	Read-only	Rate (/s) counter for sslbetotrsa3072keyexchanges
sslbetotrsa4096keyexchanges	<Double>	Read-only	Number of back-end RSA 4096-bit key exchanges on the Citrix ADC.
sslbersa4096keyexchangesrate	<Double>	Read-only	Rate (/s) counter for sslbetotrsa4096keyexchanges
sslbetotdh512keyexchanges	<Double>	Read-only	Number of back-end DH 512-bit key exchanges on the Citrix ADC.
sslbedh512keyexchangesrate	<Double>	Read-only	Rate (/s) counter for sslbetotdh512keyexchanges
sslbetotdh1024keyexchanges	<Double>	Read-only	Number of back-end DH 1024-bit key exchanges on the Citrix ADC.
sslbedh1024keyexchangesrate	<Double>	Read-only	Rate (/s) counter for sslbetotdh1024keyexchanges
sslbetotdh2048keyexchanges	<Double>	Read-only	Number of back-end DH 2048-bit key exchanges on the Citrix ADC.
sslbedh2048keyexchangesrate	<Double>	Read-only	Rate (/s) counter for sslbetotdh2048keyexchanges

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
sslbetotdh3072keyexchanges	<Double>	Read-only	Number of back-end DH 3072-bit key exchanges on the Citrix ADC.
sslbedh3072keyexchangesrate	<Double>	Read-only	Rate (/s) counter for sslbetotdh3072keyexchanges
sslbetotdh4096keyexchanges	<Double>	Read-only	Number of back-end DH 4096-bit key exchanges on the Citrix ADC.
sslbedh4096keyexchangesrate	<Double>	Read-only	Rate (/s) counter for sslbetotdh4096keyexchanges
sslbetotecdhecurve521	<Double>	Read-only	Number of back-end ECDHE 521 curve Key exchanges on the Citrix ADC.
sslbeecdhecurve521rate	<Double>	Read-only	Rate (/s) counter for sslbetotecdhecurve521
sslbetotecdhecurve384	<Double>	Read-only	Number of back-end ECDHE 384 curve Key exchanges on the Citrix ADC.
sslbeecdhecurve384rate	<Double>	Read-only	Rate (/s) counter for sslbetotecdhecurve384
sslbetotecdhecurve256	<Double>	Read-only	Number of back-end ECDHE 256 curve Key exchanges on the Citrix ADC.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
sslbeecdhecurve256rate	<Double>	Read-only	Rate (/s) counter for sslbetotecdhecurve256
sslbetotecdhecurve224	<Double>	Read-only	Number of back-end ECDHE 224 curve Key exchanges on the Citrix ADC.
sslbeecdhecurve224rate	<Double>	Read-only	Rate (/s) counter for sslbetotecdhecurve224
sslbetotecdhecurve25519	<Double>	Read-only	Number of back-end ECDHE 25519 curve Key exchanges on the Citrix ADC.
sslbeecdhecurve25519rate	<Double>	Read-only	Rate (/s) counter for sslbetotecdhecurve25519
sslbetot40bitrc4ciphers	<Double>	Read-only	Number of back-end RC4 40-bit cipher encryptions on the Citrix ADC.
sslbe40bitrc4ciphersrate	<Double>	Read-only	Rate (/s) counter for sslbetot40bitrc4ciphers
sslbetot56bitrc4ciphers	<Double>	Read-only	Number of back-end RC4 56-bit cipher encryptions on the Citrix ADC.
sslbe56bitrc4ciphersrate	<Double>	Read-only	Rate (/s) counter for sslbetot56bitrc4ciphers

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
sslbetot64bitrc4ciphers	<Double>	Read-only	Number of back-end RC4 64-bit cipher encryptions on the Citrix ADC.
sslbe64bitrc4ciphersrate	<Double>	Read-only	Rate (/s) counter for sslbetot64bitrc4ciphers
sslbetot128bitrc4ciphers	<Double>	Read-only	Number of back-end RC4 128-bit cipher encryptions on the Citrix ADC.
sslbe128bitrc4ciphersrate	<Double>	Read-only	Rate (/s) counter for sslbetot128bitrc4ciphers
sslbetot40bitdesciphers	<Double>	Read-only	Number of back-end DES 40-bit cipher encryptions on the Citrix ADC.
sslbe40bitdesciphersrate	<Double>	Read-only	Rate (/s) counter for sslbetot40bitdesciphers
sslbetot56bitdesciphers	<Double>	Read-only	Number of back-end DES 56-bit cipher encryptions on the Citrix ADC.
sslbe56bitdesciphersrate	<Double>	Read-only	Rate (/s) counter for sslbetot56bitdesciphers
sslbetot168bit3desciphers	<Double>	Read-only	Number of back-end 3DES 168-bit cipher encryptions on the Citrix ADC.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
sslbe168bit3desciphersrate	<Double>	Read-only	Rate (/s) counter for sslbetot168bit3desciphers
ssltotbkendcipheraes128	<Double>	Read-only	Back-end AES 128-bit cipher encryptions on the Citrix ADC.
sslbkendcipheraes128rate	<Double>	Read-only	Rate (/s) counter for ssltotbkendcipheraes128
ssltotbkendcipheraes256	<Double>	Read-only	Back-end AES 256-bit cipher encryptions on the Citrix ADC.
sslbkendcipheraes256rate	<Double>	Read-only	Rate (/s) counter for ssltotbkendcipheraes256
sslbetot40bitrc2ciphers	<Double>	Read-only	Number of back-end RC2 40-bit cipher encryptions on the Citrix ADC.
sslbe40bitrc2ciphersrate	<Double>	Read-only	Rate (/s) counter for sslbetot40bitrc2ciphers
sslbetot56bitrc2ciphers	<Double>	Read-only	Number of back-end RC2 56-bit cipher encryptions on the Citrix ADC.
sslbe56bitrc2ciphersrate	<Double>	Read-only	Rate (/s) counter for sslbetot56bitrc2ciphers
sslbetot128bitrc2ciphers	<Double>	Read-only	Number of back-end RC2 128-bit cipher

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			encryptions on the Citrix ADC.
sslbe128bitrc2ciphersrate	<Double>	Read-only	Rate (/s) counter for sslbetot128bitrc2ciphers
ssltotbkendcipheraesgcm128	<Double>	Read-only	Back-end AES-GCM 128-bit cipher encryptions on the Citrix ADC.
sslbkendcipheraesgcm128rate	<Double>	Read-only	Rate (/s) counter for ssltotbkendcipheraesgcm128
ssltotbkendcipheraesgcm256	<Double>	Read-only	Back-end AES-GCM 256-bit cipher encryptions on the Citrix ADC .
sslbkendcipheraesgcm256rate	<Double>	Read-only	Rate (/s) counter for ssltotbkendcipheraesgcm256
sslbetotnullciphers	<Double>	Read-only	Number of back-end null cipher encryptions on the Citrix ADC.
sslbenullciphersrate	<Double>	Read-only	Rate (/s) counter for sslbetotnullciphers
sslbetotmd5mac	<Double>	Read-only	Number of back-end MD5 hashes on the Citrix ADC.
sslbemd5macrate	<Double>	Read-only	Rate (/s) counter for sslbetotmd5mac

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
sslbetotshamac	<Double>	Read-only	Number of back-end SHA hashes on the Citrix ADC.
sslbeshamacrate	<Double>	Read-only	Rate (/s) counter for sslbetotshamac
sslbetotsha256mac	<Double>	Read-only	Number of back-end SHA256 hashes on the Citrix ADC.
sslbesha256macrate	<Double>	Read-only	Rate (/s) counter for sslbetotsha256mac
sslbetotsha384mac	<Double>	Read-only	Number of back-end SHA384 hashes on the Citrix ADC.
sslbesha384macrate	<Double>	Read-only	Rate (/s) counter for sslbetotsha384mac
sslbetotsslv3handshakes	<Double>	Read-only	Number of back-end SSLv3 handshakes on the Citrix ADC.
sslbesslv3handshakesrate	<Double>	Read-only	Rate (/s) counter for sslbetotsslv3handshakes
sslbetottlsv1handshakes	<Double>	Read-only	Number of back-end TLSv1 handshakes on the Citrix ADC.
sslbetlsv1handshakesrate	<Double>	Read-only	Rate (/s) counter for sslbetottlsv1handshakes
sslbetottlsv11handshakes	<Double>	Read-only	Number of back-end TLSv1.1 handshakes on the Citrix ADC.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
sslbetlsv11handshakesrate	<Double>	Read-only	Rate (/s) counter for sslbetottlsv11handshakes
sslbetottlsv12handshakes	<Double>	Read-only	Number of back-end TLSv1.2 handshakes on the Citrix ADC.
sslbetlsv12handshakesrate	<Double>	Read-only	Rate (/s) counter for sslbetottlsv12handshakes
sslbetottlsv13handshakes	<Double>	Read-only	Number of back-end TLSv1.3 handshakes on the Citrix ADC.
sslbetlsv13handshakesrate	<Double>	Read-only	Rate (/s) counter for sslbetottlsv13handshakes
sslbetotdtlsv1handshakes	<Double>	Read-only	Number of back-end DTLSv1 handshakes on the Citrix ADC.
sslbedtlsv1handshakesrate	<Double>	Read-only	Rate (/s) counter for sslbetotdtlsv1handshakes
sslbetotdtlsv12handshakes	<Double>	Read-only	Number of back-end DTLSv1.2 handshakes on the Citrix ADC.
sslbedtlsv12handshakesrate	<Double>	Read-only	Rate (/s) counter for sslbetotdtlsv12handshakes
sslbetotsslv3clientauthentications	<Double>	Read-only	Number of back-end SSLv3 client authentications on the Citrix ADC.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
sslbesslv3clientauthenticationsrate	<Double>	Read-only	Rate (/s) counter for sslbetotsslv3clientauthentications
sslbetottlsv1clientauthentications	<Double>	Read-only	Number of back-end TLSv1 client authentications on the Citrix ADC.
sslbetlsv1clientauthenticationsrate	<Double>	Read-only	Rate (/s) counter for sslbetottlsv1clientauthentications
sslbetottlsv11clientauthentications	<Double>	Read-only	Number of back-end TLSv1.1 client authentications on the Citrix ADC.
sslbetlsv11clientauthenticationsrate	<Double>	Read-only	Rate (/s) counter for sslbetottlsv11clientauthentications
sslbetottlsv12clientauthentications	<Double>	Read-only	Number of back-end TLSv1.2 client authentications on the Citrix ADC.
sslbetlsv12clientauthenticationsrate	<Double>	Read-only	Rate (/s) counter for sslbetottlsv12clientauthentications
sslbetottlsv13clientauthentications	<Double>	Read-only	Number of back-end TLSv1.3 client authentications on the Citrix ADC.
sslbetlsv13clientauthenticationsrate	<Double>	Read-only	Rate (/s) counter for sslbetottlsv13clientauthentications

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
sslbetotdtlsv1clientauthentications	<Double>	Read-only	Number of back-end DTLSv1 client authentications on the Citrix ADC.
sslbedtlsv1clientauthenticationsrate	<Double>	Read-only	Rate (/s) counter for sslbetotdtlsv1clientauthentications
sslbetotdtlsv12clientauthentications	<Double>	Read-only	Number of back-end DTLSv1.2 client authentications on the Citrix ADC.
sslbedtlsv12clientauthenticationsrate	<Double>	Read-only	Rate (/s) counter for sslbetotdtlsv12clientauthentications
sslbetotrsaauthorizations	<Double>	Read-only	Number of back-end RSA authentications on the Citrix ADC.
sslbersaauthorizationsrate	<Double>	Read-only	Rate (/s) counter for sslbetotrsaauthorizations
sslbetotdhauthorizations	<Double>	Read-only	Number of back-end DH authentications on the Citrix ADC.
sslbedhauthorizationsrate	<Double>	Read-only	Rate (/s) counter for sslbetotdhauthorizations
sslbetotdssauthorizations	<Double>	Read-only	Number of back-end DSS authentications on the Citrix ADC.
sslbedssauthorizationsrate	<Double>	Read-only	Rate (/s) counter for sslbetotdssauthorizations

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
sslbetotecdsaauthorizations	<Double>	Read-only	Number of back-end ECDSA authentications on the Citrix ADC.
sslbeecdsaauthorizationsrate	<Double>	Read-only	Rate (/s) counter for sslbetotecdsaauthorizations
sslbetotnullauthorizations	<Double>	Read-only	Number of back-end null authentications on the Citrix ADC.
sslbenullauthorizationsrate	<Double>	Read-only	Rate (/s) counter for sslbetotnullauthorizations
ssltotoffloadrsakeyexchanges	<Double>	Read-only	Number of RSA key exchanges offloaded to the cryptography card.
sslloffloadrsakeyexchangesrate	<Double>	Read-only	Rate (/s) counter for ssltotoffloadrsakeyexchanges
ssltotoffloadsignrsa	<Double>	Read-only	Number of RSA sign operations offloaded to the cryptography card.
sslloffloadsignrsarate	<Double>	Read-only	Rate (/s) counter for ssltotoffloadsignrsa
ssltotoffloaddhkeyexchanges	<Double>	Read-only	Number of DH key exchanges offloaded to the cryptography card.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ssloffloaddhkeyexchangesrate	<Double>	Read-only	Rate (/s) counter for ssltotoffloaddhkeyexchanges
ssltotoffloadbulkrc4	<Double>	Read-only	Number of RC4 encryptions offloaded to the cryptography card.
ssloffloadbulkrc4rate	<Double>	Read-only	Rate (/s) counter for ssltotoffloadbulkrc4
ssltotoffloadbulkdes	<Double>	Read-only	Number of DES encryptions offloaded to the cryptography card.
ssloffloadbulkdesrate	<Double>	Read-only	Rate (/s) counter for ssltotoffloadbulkdes
ssltotoffloadbulkaes	<Double>	Read-only	Number of AES encryptions offloaded to the cryptography card.
ssloffloadbulkaesrate	<Double>	Read-only	Rate (/s) counter for ssltotoffloadbulkaes
ssltotoffloadbulkaesgcm128	<Double>	Read-only	Number of AES-GCM 128-bit encryptions offloaded to the cryptography card.
ssloffloadbulkaesgcm128rate	<Double>	Read-only	Rate (/s) counter for ssltotoffloadbulkaesgcm128
ssltotoffloadbulkaesgcm256	<Double>	Read-only	Number of AES-GCM 256-bit encryptions

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			offloaded to the cryptography card.
ssloffloadbulkaesgcm256rate	<Double>	Read-only	Rate (/s) counter for ssltotoffloadbulkaesgcm256
ssltotenchw	<Double>	Read-only	Number of bytes encrypted in hardware.
sslenchwrate	<Double>	Read-only	Rate (/s) counter for ssltotenchw
ssltotencsw	<Double>	Read-only	Number of bytes encrypted in software.
sslencswrate	<Double>	Read-only	Rate (/s) counter for ssltotencsw
ssltotencfe	<Double>	Read-only	Number of bytes encrypted on the front-end.
sslencferate	<Double>	Read-only	Rate (/s) counter for ssltotencfe
ssltothwencfe	<Double>	Read-only	Number of bytes encrypted in hardware on the front-end.
sslhwencferate	<Double>	Read-only	Rate (/s) counter for ssltothwencfe
ssltotswencfe	<Double>	Read-only	Number of bytes encrypted in software on the front-end.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
sslswencferate	<Double>	Read-only	Rate (/s) counter for ssltotswencfe
ssltotencbe	<Double>	Read-only	Number of bytes encrypted on the back-end.
sslencberate	<Double>	Read-only	Rate (/s) counter for ssltotencbe
ssltothwencbe	<Double>	Read-only	Number of bytes encrypted in hardware on the back-end.
sslhwencberate	<Double>	Read-only	Rate (/s) counter for ssltothwencbe
ssltotswencbe	<Double>	Read-only	Number of bytes encrypted in software on the back-end.
sslswencberate	<Double>	Read-only	Rate (/s) counter for ssltotswencbe
ssltotdechw	<Double>	Read-only	Number of bytes decrypted in hardware.
ssldechwrate	<Double>	Read-only	Rate (/s) counter for ssltotdechw
ssltotdecsw	<Double>	Read-only	Number of bytes decrypted in software.
ssldecswrate	<Double>	Read-only	Rate (/s) counter for ssltotdecsw

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ssltotdecfe	<Double>	Read-only	Number of bytes decrypted on the front-end.
ssldecferate	<Double>	Read-only	Rate (/s) counter for ssltotdecfe
ssltothwdecfe	<Double>	Read-only	Number of bytes decrypted in hardware on the front-end.
sslhwdecferate	<Double>	Read-only	Rate (/s) counter for ssltothwdecfe
ssltotswdecfe	<Double>	Read-only	Number of bytes decrypted in software on the front-end.
sslswdecferate	<Double>	Read-only	Rate (/s) counter for ssltotswdecfe
ssltotdecbe	<Double>	Read-only	Number of bytes decrypted on the back-end.
ssldecberate	<Double>	Read-only	Rate (/s) counter for ssltotdecbe
ssltothwdecbe	<Double>	Read-only	Number of bytes decrypted in hardware on the back-end.
sslhwdecberate	<Double>	Read-only	Rate (/s) counter for ssltothwdecbe
ssltotswdecbe	<Double>	Read-only	Number of bytes decrypted in

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			software on the back-end
sslswdecberate	<Double>	Read-only	Rate (/s) counter for ssltotswdecbe
sslcursslinfospcbinusecount	<Double>	Read-only	Number of SPCB in use.
sslcursslinfospcbinusecountrate	<Double>	Read-only	Rate (/s) counter for sslcursslinfospcbinusecount
sslcursessions	<Double>	Read-only	Number of active SSL sessions on the Citrix ADC.
sslcursessionsrate	<Double>	Read-only	Rate (/s) counter for sslcursessions
sslcurqsize	<Double>	Read-only	Current queue size
sslcurqsizerate	<Double>	Read-only	Rate (/s) counter for sslcurqsize
sslcursslinfonscardinqcount	<Double>	Read-only	Number of current SSL card InQ count.
sslcursslinfonscardinqcountrate	<Double>	Read-only	Rate (/s) counter for sslcursslinfonscardinqcount
sslcursslinfocardinblkq	<Double>	Read-only	Number of current SSL card In BulkQ count.
sslcursslinfocardinblkqrate	<Double>	Read-only	Rate (/s) counter for sslcursslinfocardinblkq

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
sslcursslinfocardinkeyq	<Double>	Read-only	Number of current SSL card In KeyQ count.
sslcursslinfocardinkeyqrate	<Double>	Read-only	Rate (/s) counter for sslcursslinfocardinkeyq
sslbemaxmultiplexedsessions	<Double>	Read-only	Number of back-end SSL sessions reused on the Citrix ADC.
sslbemaxmultiplexedsessionsrate	<Double>	Read-only	Rate (/s) counter for sslbemaxmultiplexedsessions
ssltot128bitideaciphers	<Double>	Read-only	Number of IDEA 128-bit cipher encryptions on the Citrix ADC.
ssl128bitideaciphersrate	<Double>	Read-only	Rate (/s) counter for ssltot128bitideaciphers
sslbetot128bitideaciphers	<Double>	Read-only	Number of back-end IDEA 128-bit cipher encryptions on the Citrix ADC.
sslbe128bitideaciphersrate	<Double>	Read-only	Rate (/s) counter for sslbetot128bitideaciphers

Operations

(click to see Properties)

- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/ssl **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/ssl? **args=detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get ssl resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/ssl? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "ssl": [ {

"ssltotdtlsv12transactions":<Double_value>,

"sslbersa3072keyexchangesrate":<Double_value>,

"ssltotencbe":<Double_value>,

"ssltotoffloadbulkrc4":<Double_value>,

"sslecdsap256cryptoutilizationstat":<Double_value>,

"sslbe168bit3desciphersrate":<Double_value>,

"sslbemd5macrate":<Double_value>,

"ssltot40bitrc4ciphers":<Double_value>,

"sslbetottlsv11clientauthentications":<Double_value>,

"ssltotbkendcipheraesgcm256":<Double_value>,

"sslbenullciphersrate":<Double_value>,

"sslbetlsv13sessionsrate":<Double_value>,

"sslbetottlsv11sessions":<Double_value>,

"sslbetot56bitdesciphers":<Double_value>,

"sslbetotsessionmultiplexattempts":<Double_value>,
```

```
"sslbkendtlsv11renegorate":<Double_value>,

"ssldh512keyexchangesrate":<Double_value>,

"sslasymdhcryptoutilizationstat":<Double_value>,

"sslbe128bitideaciphersrate":<Double_value>,

"sslcursessions":<Double_value>,

"ssltotmd5mac":<Double_value>,

"ssltot56bitdesciphers":<Double_value>,

"sslbeshamacrate":<Double_value>,

"ssltot40bitrc2ciphers":<Double_value>,

"sslbetotrsa2048keyexchanges":<Double_value>,

"ssltlsv1sessionsrate":<Double_value>,

"sslecdsap224cryptoutilizationstat":<Double_value>,

"ssltottlsv13sessions":<Double_value>,

"sslcursslinfocardinblkqrate":<Double_value>,

"ssltotcipheraes256":<Double_value>,

"sslbedh2048keyexchangesrate":<Double_value>,

"sslbeecdsaauthorizationsrate":<Double_value>,

"ssltotbkendcipheraes128":<Double_value>,

"sslcursslinfonscardinqcountrate":<Double_value>,

"ssltotbkendtlsv12renego":<Double_value>,

"sslcipheraes128rate":<Double_value>,

"sslecdsaauthorizationsrate":<Double_value>,
```

```
"sslbe40bitdesciphersrate":<Double_value>,

"ssltot128bitrc4ciphers":<Double_value>,

"sslrsa512keyexchangesrate":<Double_value>,

"sslloffloadbulkaesgcm256rate":<Double_value>,

"sslbedh4096keyexchangesrate":<Double_value>,

"ssltottlsv11clientauthentications":<Double_value>,

"ssldtlsv1sessionsrate":<Double_value>,

"ssltotdtlsv12sessions":<Double_value>,

"sslcursslinfospcbinusecountrate":<Double_value>,

"sslbetotecdhecurve256":<Double_value>,

"ssl64bitrc4ciphersrate":<Double_value>,

"sslcardssecondary":<Double_value>,

"sslrsaauthorizationsrate":<Double_value>,

"sslbemaxmultiplexedsessions":<Double_value>,

"ssltlsv1renegsessionsrate":<Double_value>,

"ssltotoffloadbulkaes":<Double_value>,

"sslbetot40bitrc2ciphers":<Double_value>,

"sslasymrsa1kcryptoutilizationstat":<Double_value>,

"sslbetottlsv13clientauthentications":<Double_value>,

"ssltotoffloadbulkaesgcm256":<Double_value>,

"sslsslv3handshakesrate":<Double_value>,

"ssltotecdhe224keyexchanges":<Double_value>,
```

```
"ssl168bit3desciphersrate":<Double_value>,

"ssltotdecfe":<Double_value>,

"sslswdecberate":<Double_value>,

"sslbetotecdsaauthorizations":<Double_value>,

"sslbesslv3handshakesrate":<Double_value>,

"sslasymecdhcryptoutilizationstat":<Double_value>,

"ssltotdhauthorizations":<Double_value>,

"sslbedssauthorizationsrate":<Double_value>,

"sslbedhauthorizationsrate":<Double_value>,

"sslhwdecfesecondaryrate":<Double_value>,

"ssltotbkendtlsvlrenego":<Double_value>,

"ssltotsslserverinrecords":<Double_value>,

"sslbetotrsa3072keyexchanges":<Double_value>,

"ssltotdtlsv1handshakes":<Double_value>,

"ssl128bitrc2ciphersrate":<Double_value>,

"sslbkendsessionrenegotiaterate":<Double_value>,

"ssltotoffloaddhkeyexchanges":<Double_value>,

"sslbetotdh2048keyexchanges":<Double_value>,

"ssl40bitdesciphersrate":<Double_value>,

"ssl56bitrc2ciphersrate":<Double_value>,

"sslcardstatus":<Double_value>,

"ssltlsv13handshakesrate":<Double_value>,
```

```
"sslbkendtlsvlrenegorate":<Double_value>,

"sslbkendcipheraesgcm256rate":<Double_value>,

"ssltotrsa4096keyexchanges":<Double_value>,

"ssltottlsv12transactions":<Double_value>,

"sslbersa512keyexchangesrate":<Double_value>,

"sslbeecdhecurve521rate":<Double_value>,

"sslloffloadbulkaesrate":<Double_value>,

"ssltlsv12handshakesrate":<Double_value>,

"sslbetotsessions":<Double_value>,

"sslsessionmissrate":<Double_value>,

"sslhwdecberate":<Double_value>,

"sslbetotdhauthorizations":<Double_value>,

"sslmd5macrate":<Double_value>,

"sslcards":<Double_value>,

"sslbetot168bit3desciphers":<Double_value>,

"ssltransactionsrate":<Double_value>,

"sslbetlsv13handshakesrate":<Double_value>,

"ssldtlsv1renegsessionsrate":<Double_value>,

"sslbetotdtlsv12clientauthentications":<Double_value>,

"sslbetlsv1clientauthenticationsrate":<Double_value>,

"sslbetotdh1024keyexchanges":<Double_value>,

"sslbetlsv1handshakesrate":<Double_value>,
```

```
"sslasymrsaotherscryptoutilizationstat":<Double_value>,

"ssltotecdhetransactions":<Double_value>,

"sslbetottlsv12clientauthentications":<Double_value>,

"ssltlsv12renegsessionsrate":<Double_value>,

"sslecdhp521cryptoutilizationstat":<Double_value>,

"ssltotbkenddtlsvlrenego":<Double_value>,

"sslnewsessionsrate":<Double_value>,

"sslbedtlsv1clientauthenticationsrate":<Double_value>,

"ssldecswrate":<Double_value>,

"ssltlsv1handshakesrate":<Double_value>,

"ssltlsv11transactionsrate":<Double_value>,

"ssltotsslv3sessions":<Double_value>,

"ssltotnewsessions":<Double_value>,

"ssltot128bitrc2ciphers":<Double_value>,

"ssl128bitrc4ciphersrate":<Double_value>,

"sslbetlsv11handshakesrate":<Double_value>,

"sslenchwrate":<Double_value>,

"sslbetotrsa4096keyexchanges":<Double_value>,

"sslecdhp384cryptoutilizationstat":<Double_value>,

"ssltotdecbe":<Double_value>,

"ssltotrsa3072keyexchanges":<Double_value>,

"sslbetot40bitrc4ciphers":<Double_value>,
```

```
"sslbetotsha384mac":<Double_value>,

"sslbetottlsv13handshakes":<Double_value>,

"sslbkendcipheraesgcm128rate":<Double_value>,

"ssltotdtlsv1sessions":<Double_value>,

"ssltotcipheraes128":<Double_value>,

"sslnullauthorizationsrate":<Double_value>,

"ssltotnullauthorizations":<Double_value>,

"sslbedtlsv1handshakesrate":<Double_value>,

"ssltotdtlsv12clientauthentications":<Double_value>,

"sslbe56bitrc2ciphersrate":<Double_value>,

"sslecdhe224keyexchangesrate":<Double_value>,

"ssltlsv1clientauthenticationsrate":<Double_value>,

"ssltottlsv1sessions":<Double_value>,

"ssl40bitrc4ciphersrate":<Double_value>,

"sslbetot128bitrc4ciphers":<Double_value>,

"sslbetotsslv3clientauthentications":<Double_value>,

"sslenchwsecondaryrate":<Double_value>,

"ssltotsessions":<Double_value>,

"sslbetotdtlsv12sessions":<Double_value>,

"sslbe56bitrc4ciphersrate":<Double_value>,

"sslhwencbesecondaryrate":<Double_value>,

"sslshamacrate":<Double_value>,
```

```
"sslbetottlsv12sessions":<Double_value>,

"ssltot128bitideaciphers":<Double_value>,

"ssltotencfe":<Double_value>,

"sslbkendtlsv12renegorate":<Double_value>,

"sslsessionhitsrate":<Double_value>,

"ssltotrsa1024keyexchanges":<Double_value>,

"sslrsa3072keyexchangesrate":<Double_value>,

"ssltlsv11handshakesrate":<Double_value>,

"sslcryptoutilizationstat":<Double_value>,

"sslsessionsrate":<Double_value>,

"sslbetotmd5mac":<Double_value>,

"sslbetotshamac":<Double_value>,

"ssldtlsv12handshakesrate":<Double_value>,

"ssldechwrate":<Double_value>,

"sslbetotrsa512keyexchanges":<Double_value>,

"sslhwencferate":<Double_value>,

"ssltotsslv3transactions":<Double_value>,

"ssltotdh2048keyexchanges":<Double_value>,

"ssltottlsv13handshakes":<Double_value>,

"ssltotoffloadbulkdes":<Double_value>,

"ssltot128bitaesgcmciphers":<Double_value>,

"sslcryptoutilizationcph":<Double_value>,
```

```
"ssldhauthorizationsrate":<Double_value>,

"sslencswrate":<Double_value>,

"sslecdsap384cryptoutilizationstat":<Double_value>,

"sslsslv3sessionsrate":<Double_value>,

"sslbesha256macrate":<Double_value>,

"ssltottlsv11transactions":<Double_value>,

"sslcryptoutilizationath":<Double_value>,

"sslbe128bitrc4ciphersrate":<Double_value>,

"sslcursslinfospcbinusecount":<Double_value>,

"sslloffloadbulkdesrate":<Double_value>,

"ssl128bitideaciphersrate":<Double_value>,

"sslbkendcipheraes256rate":<Double_value>,

"sslecdhe256keyexchangesrate":<Double_value>,

"ssldtlsv12clientauthenticationsrate":<Double_value>,

"sslbetotrsa1024keyexchanges":<Double_value>,

"ssldechwsecondaryrate":<Double_value>,

"sslsymcryptoutilizationstat":<Double_value>,

"ssltottlsv1transactions":<Double_value>,

"sslasymrsa2kcryptoutilizationstat":<Double_value>,

"ssl256bitaesgcmciphersrate":<Double_value>,

"sslecdhx25519cryptoutilizationstat":<Double_value>,

"sslbetotdtlsv1sessions":<Double_value>,
```

```
"ssltotdtlsv12handshakes":<Double_value>,

"sslswencferate":<Double_value>,

"ssltotecdsaauthorizations":<Double_value>,

"ssltlsv11clientauthenticationsrate":<Double_value>,

"ssltot168bit3desciphers":<Double_value>,

"sslbedtlsv12sessionsrate":<Double_value>,

"sslsslv3renegsessionsrate":<Double_value>,

"sslbetotecdhecurve521":<Double_value>,

"sslbetotecdhecurve384":<Double_value>,

"ssltlsv13sessionsrate":<Double_value>,

"sslbetotdh3072keyexchanges":<Double_value>,

"ssltotsha256mac":<Double_value>,

"sslbetottlsv1clientauthentications":<Double_value>,

"sslcryptoutilizationstat2nd":<Double_value>,

"ssltotswdecfe":<Double_value>,

"sslcurqsizerate":<Double_value>,

"ssltottlsv11sessions":<Double_value>,

"sslswencberate":<Double_value>,

"ssltotdh1024keyexchanges":<Double_value>,

"ssltotrenegsessions":<Double_value>,

"ssltotoffloadrsakeyexchanges":<Double_value>,

"ssltothwencbesecondary":<Double_value>,
```

```
"sslsha384macrate":<Double_value>,

"sslbetlsv13clientauthenticationsrate":<Double_value>,

"sslbetlsv12clientauthenticationsrate":<Double_value>,

"ssltotrsa512keyexchanges":<Double_value>,

"ssltottlsv1renegsessions":<Double_value>,

"sslbeecdhecurve224rate":<Double_value>,

"ssltotecdhe256keyexchanges":<Double_value>,

"ssltot256bitaesgcmciphers":<Double_value>,

"ssltlsv12sessionsrate":<Double_value>,

"ssltotenc":<Double_value>,

"ssldtlsv12transactionsrate":<Double_value>,

"ssltotdechwsecondary":<Double_value>,

"ssltotdecsw":<Double_value>,

"ssltotdh4096keyexchanges":<Double_value>,

"ssltotdssauthorizations":<Double_value>,

"sslbetotecdhecurve224":<Double_value>,

"sslbeecdhecurve25519rate":<Double_value>,

"ssldecrate":<Double_value>,

"sslnullciphersrate":<Double_value>,

"sslhwencfesecondaryrate":<Double_value>,

"sslsslv3clientauthenticationsrate":<Double_value>,

"sslecdhp224cryptoutilizationstat":<Double_value>,
```

```
"ssltotsessionhits":<Double_value>,

"ssltotdh3072keyexchanges":<Double_value>,

"ssltot56bitrc4ciphers":<Double_value>,

"ssltotrsaauthorizations":<Double_value>,

"ssltotdechw":<Double_value>,

"sslbetotdssauthorizations":<Double_value>,

"sslbesslv3sessionsrate":<Double_value>,

"ssltotswencbe":<Double_value>,

"sslrsa2048keyexchangesrate":<Double_value>,

"sslbedtlsv1sessionsrate":<Double_value>,

"ssltotbkendcipheraesgcm128":<Double_value>,

"sslbetot56bitrc2ciphers":<Double_value>,

"ssltot40bitdesciphers":<Double_value>,

"ssltothwdecfesecondary":<Double_value>,

"sslhwencberate":<Double_value>,

"sslbetotrsaauthorizations":<Double_value>,

"ssltotsslv3renegsessions":<Double_value>,

"sslnumcardsup":<Double_value>,

"sslbedh1024keyexchangesrate":<Double_value>,

"ssldecberate":<Double_value>,

"ssltot56bitrc2ciphers":<Double_value>,

"ssltotbkendsslv3renego":<Double_value>,
```

```
"ssltottlsv11renegsessions":<Double_value>,

"sslbesslv3clientauthenticationsrate":<Double_value>,

"sslbetotdh512keyexchanges":<Double_value>,

"sslbetotdtlsv1clientauthentications":<Double_value>,

"sslbetot128bitrc2ciphers":<Double_value>,

"sslbersa4096keyexchangesrate":<Double_value>,

"sslloffloadbulkaesgcm128rate":<Double_value>,

"sslbetottlsv11handshakes":<Double_value>,

"sslecdsap521cryptoutilizationstat":<Double_value>,

"ssltotecdhe521keyexchanges":<Double_value>,

"ssltottlsv12handshakes":<Double_value>,

"sslbemaxmultiplexedsessionsrate":<Double_value>,

"sslnumcardsupsecondary":<Double_value>,

"ssltothwdecfe":<Double_value>,

"sslbetlsv12sessionsrate":<Double_value>,

"sslbesessionmultiplexattemptsrate":<Double_value>,

"ssldtlsv1handshakesrate":<Double_value>,

"ssltotbkendsessionrenegotiate":<Double_value>,

"ssltotdtlsv1transactions":<Double_value>,

"sslasymcryptoutilizationstat":<Double_value>,

"sslbkendcipheraes128rate":<Double_value>,

"sslbetotsessionmultiplexattemptfails":<Double_value>,
```

```
"ssldssauthorizationsrate":<Double_value>,

"sslasymecdsacryptoutilizationstat":<Double_value>,

"sslbersa2048keyexchangesrate":<Double_value>,

"ssltotsha384mac":<Double_value>,

"ssl56bitrc4ciphersrate":<Double_value>,

"sslcursslinfocardinblkq":<Double_value>,

"ssltlsv1transactionsrate":<Double_value>,

"sslcursslinfocardinkeyq":<Double_value>,

"sslbeecdhecurve256rate":<Double_value>,

"sslencrate":<Double_value>,

"ssltlsv12clientauthenticationsrate":<Double_value>,

"sslecdhe384keyexchangesrate":<Double_value>,

"sslbedtlsv12clientauthenticationsrate":<Double_value>,

"sslcursessionsrate":<Double_value>,

"sslbetot40bitdesciphers":<Double_value>,

"sslbe56bitdesciphersrate":<Double_value>,

"sslasymrsacryptoutilizationstat":<Double_value>,

"ssltothwencbe":<Double_value>,

"sslbetotdtlsv12handshakes":<Double_value>,

"sslcryptoutilizationucs":<Double_value>,

"sslbetotsslv3sessions":<Double_value>,

"sslencberate":<Double_value>,
```

```
"sslsslserverinrecordsrate":<Double_value>,

"sslbenullauthorizationsrate":<Double_value>,

"ssloffloadbulkrc4rate":<Double_value>,

"ssltotpqcx25519mlkem768keyexchanges":<Double_value>,

"sslbetottlsv1sessions":<Double_value>,

"ssloffloadsignrsarate":<Double_value>,

"ssltotsessionmiss":<Double_value>,

"ssltotdtlsv12renegsessions":<Double_value>,

"ssltothwencfe":<Double_value>,

"ssltotsslv3handshakes":<Double_value>,

"ssltottlsv1clientauthentications":<Double_value>,

"sslbetottlsv12handshakes":<Double_value>,

"sslhwdecbesecondaryrate":<Double_value>,

"ssltotecdhe384keyexchanges":<Double_value>,

"ssldtlsv1transactionsrate":<Double_value>,

"sslcursslinfocardinkeyqrate":<Double_value>,

"sslbetot128bitideaciphers":<Double_value>,

"ssldh4096keyexchangesrate":<Double_value>,

"sslhwdecferate":<Double_value>,

"sslcryptoutilizationasym":<Double_value>,

"ssl128bitaesgcmciphersrate":<Double_value>,

"ssltotnullciphers":<Double_value>,
```

```
"sslbe40bitrc4ciphersrate":<Double_value>,

"ssltottlsv12sessions":<Double_value>,

"ssltothwdecbe":<Double_value>,

"sslbkenddtlsvlrenegorate":<Double_value>,

"ssldtlsv1clientauthenticationsrate":<Double_value>,

"ssltottlsv1handshakes":<Double_value>,

"ssloffloaddhkeyexchangesrate":<Double_value>,

"sslbetotdh4096keyexchanges":<Double_value>,

"sslbetlsv12handshakesrate":<Double_value>,

"sslbetotsha256mac":<Double_value>,

"sslrsa4096keyexchangesrate":<Double_value>,

"ssltlsv13clientauthenticationsrate":<Double_value>,

"ssltlsv11sessionsrate":<Double_value>,

"ssltotbkendtlsv11renego":<Double_value>,

"sslbedh3072keyexchangesrate":<Double_value>,

"ssldtlsv12sessionsrate":<Double_value>,

"sslbetotecdhecurve25519":<Double_value>,

"sslsslv3transactionsrate":<Double_value>,

"ssltotenchw":<Double_value>,

"ssloffloadrsakeyexchangesrate":<Double_value>,

"ssltottransactions":<Double_value>,

"ssldtlsv12renegsessionsrate":<Double_value>,
```

```
"sslswdecferate":<Double_value>,

"ssltot64bitrc4ciphers":<Double_value>,

"sslbe64bitrc4ciphersrate":<Double_value>,

"sslbetotsslv3handshakes":<Double_value>,

"sslecdhetransactionsrate":<Double_value>,

"sslbetlsv11sessionsrate":<Double_value>,

"sslasymrsa4kcryptoutilizationstat":<Double_value>,

"ssltotdec":<Double_value>,

"ssltotenchwsecondary":<Double_value>,

"ssltotencsw":<Double_value>,

"sslbetotsessionmultiplexattemptsuccess":<Double_value>,

"ssltlsv11renegsessionsrate":<Double_value>,

"ssldecferate":<Double_value>,

"sslenginestatus":<Double_value>,

"sslbetottlsv1handshakes":<Double_value>,

"sslbesessionmultiplexattemptsuccessrate":<Double_value>,

"sslrenegsessionsrate":<Double_value>,

"sslbetotdtlsv1handshakes":<Double_value>,

"ssl56bitdesciphersrate":<Double_value>,

"ssltotbkendcipheraes256":<Double_value>,

"sslcursslinfonscardinqcount":<Double_value>,

"sslecdhe25519keyexchangesrate":<Double_value>,
```

```
"ssl40bitrc2ciphersrate":<Double_value>,

"sslbe128bitrc2ciphersrate":<Double_value>,

"ssltotswencfe":<Double_value>,

"sslbersaauthorizationsrate":<Double_value>,

"sslbkendsslv3renegorate":<Double_value>,

"sslbetotnullciphers":<Double_value>,

"ssltothwdecbesecondary":<Double_value>,

"ssltotecdhe25519keyexchanges":<Double_value>,

"sslcipheraes256rate":<Double_value>,

"ssldh3072keyexchangesrate":<Double_value>,

"sslbesessionsrate":<Double_value>,

"ssltlsv13transactionsrate":<Double_value>,

"ssltotbkenddtlsvl2renego":<Double_value>,

"sslrsa1024keyexchangesrate":<Double_value>,

"sslbetot56bitrc4ciphers":<Double_value>,

"ssltotoffloadbulkaesgcm128":<Double_value>,

"ssltottlsv12clientauthentications":<Double_value>,

"ssldh2048keyexchangesrate":<Double_value>,

"ssltotdtlsv1renegsessions":<Double_value>,

"sslecdhp256cryptoutilizationstat":<Double_value>,

"sslbkenddtlsvl2renegorate":<Double_value>,

"ssltottlsv11handshakes":<Double_value>,
```

```
"ssltotsslv3clientauthentications":<Double_value>,

"sslbetotnullauthorizations":<Double_value>,

"sslecdhe521keyexchangesrate":<Double_value>,

"sslbetlsv11clientauthenticationsrate":<Double_value>,

"sslbetottlsv13sessions":<Double_value>,

"ssltotswdecbe":<Double_value>,

"sslpqcx25519mlkem768keyexchangesrate":<Double_value>,

"ssltotrsa2048keyexchanges":<Double_value>,

"ssltothwencfesecondary":<Double_value>,

"sslbeecdhecurve384rate":<Double_value>,

"sslbedh512keyexchangesrate":<Double_value>,

"sslbe40bitrc2ciphersrate":<Double_value>,

"sslbedtlsv12handshakesrate":<Double_value>,

"ssltottlsv13transactions":<Double_value>,

"sslbesha384macrate":<Double_value>,

"ssltotoffloadsignrsa":<Double_value>,

"sslbetlsv1sessionsrate":<Double_value>,

"sslbersa1024keyexchangesrate":<Double_value>,

"sslencferate":<Double_value>,

"ssltottlsv13clientauthentications":<Double_value>,

"sslbesessionmultiplexattemptfailsrate":<Double_value>,

"ssltottlsv12renegsessions":<Double_value>,
```

```
"ssltotshamac":<Double_value>,

"ssldh1024keyexchangesrate":<Double_value>,

"sslcurqsize":<Double_value>,

"ssltlsv12transactionsrate":<Double_value>,

"sslbetot64bitrc4ciphers":<Double_value>,

"sslsha256macrate":<Double_value>,

"ssltotdtlsv1clientauthentications":<Double_value>,

"ssltotdh512keyexchanges":<Double_value>,

"sslcryptoutilizationsymm":<Double_value>

}]}
```

sslvserver

Statistics for SSL virtual server resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
vservername	<String>	Read-write	Name of the SSL virtual server for which to show detailed statistics. Minimum length = 1
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
vslbhealth	<Double>	Read-only	Health of the vserver. This gives percentage of UP services bound to this vserver.
primaryipaddress	<String>	Read-only	IP address of the vserver
primaryport	<Integer>	Read-only	The port on which the service is running.
type	<String>	Read-only	Protocol associated with the vserver
state	<String>	Read-only	Current state of the server. There are seven possible values: UP(7), DOWN(1), UNKNOWN(2), BUSY(3), OFS(Out of Service)(4), TROFS(Transition Out of Service)(5), TROFS_DOWN(Down When going Out of Service)(8)
actsvcs	<Double>	Read-only	number of ACTIVE services bound to a vserver
ssltotclientauthsuccess	<Double>	Read-only	Number of successful client authentication on this vserver

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
sslclientauthsuccessrate	<Double>	Read-only	Rate (/s) counter for ssltotclientauthsuccess
ssltotclientauthfailure	<Double>	Read-only	Number of failure client authentication on this vserver
sslclientauthfailurerate	<Double>	Read-only	Rate (/s) counter for ssltotclientauthfailure
sslctxtotencbytes	<Double>	Read-only	Number of encrypted bytes per SSL vserver
sslctxencbytesrate	<Double>	Read-only	Rate (/s) counter for sslctxtotencbytes
sslctxtotdecbytes	<Double>	Read-only	Number of decrypted bytes per SSL vserver
sslctxdecbytesrate	<Double>	Read-only	Rate (/s) counter for sslctxtotdecbytes
sslctxtothwencbytes	<Double>	Read-only	Number of hardware encrypted bytes per SSL vserver
sslctxhwencbytesrate	<Double>	Read-only	Rate (/s) counter for sslctxtothwencbytes
sslctxtothwdec_bytes	<Double>	Read-only	Number of hw decrypted bytes per SSL vserver
sslctxhwdec_bytesrate	<Double>	Read-only	Rate (/s) counter for sslctxtothwdec_bytes
sslctxtotsessionnew	<Double>	Read-only	Number of new sessions created

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
sslctxsessionnewrate	<Double>	Read-only	Rate (/s) counter for sslctxtotsessionnew
sslctxtotsessionhits	<Double>	Read-only	Number of session hits
sslctxsessionhitsrate	<Double>	Read-only	Rate (/s) counter for sslctxtotsessionhits

Operations

(click to see Properties)

- GET (ALL)
- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/sslvserver **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/sslvserver? **args=vservername: <String_value> ,detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get sslvserver resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/sslvserver? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslvserver": [ {

"vservername":<String_value>,

"sslctxsessionhitsrate":<Double_value>,

"sslctxtotsessionnew":<Double_value>,

"sslclientauthfailurerate":<Double_value>,
```

```
"sslctxencbytesrate":<Double_value>,

"sslctxsessionnewrate":<Double_value>,

"state":<String_value>,

"sslctxdecbytesrate":<Double_value>,

"ssltotclientauthsuccess":<Double_value>,

"sslctxtotdecbytes":<Double_value>,

"type":<String_value>,

"ssltotclientauthfailure":<Double_value>,

"sslclientauthsuccessrate":<Double_value>,

"primaryipaddress":<String_value>,

"sslctxtothwencbytes":<Double_value>,

"sslctxhwencbytesrate":<Double_value>,

"primaryport":<Integer_value>,

"vslbhealth":<Double_value>,

"sslctxtotsessionhits":<Double_value>,

"actsvcs":<Double_value>,

"sslctxhwdec_bytesrate":<Double_value>,

"sslctxtothwdec_bytes":<Double_value>,

"sslctxtotencbytes":<Double_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/stat/sslvserver/ vservername_value><String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslvserver": [ {

"vservername":<String_value>,

"sslctxsessionhitsrate":<Double_value>,

"sslctxtotsessionnew":<Double_value>,

"sslclientauthfailurerate":<Double_value>,

"sslctxencbytesrate":<Double_value>,

"sslctxsessionnewrate":<Double_value>,

"state":<String_value>,

"sslctxdecbytesrate":<Double_value>,

"ssltotclientauthsuccess":<Double_value>,

"sslctxtotdecbytes":<Double_value>,

"type":<String_value>,
```

```
"ssltotclientauthfailure":<Double_value>,

"sslclientauthsuccessrate":<Double_value>,

"primaryipaddress":<String_value>,

"sslctxtothwencbytes":<Double_value>,

"sslctxhwencbytesrate":<Double_value>,

"primaryport":<Integer_value>,

"vslbhealth":<Double_value>,

"sslctxtotsessionhits":<Double_value>,

"actsvcs":<Double_value>,

"sslctxhwdec_bytesrate":<Double_value>,

"sslctxtothwdec_bytes":<Double_value>,

"sslctxtotencbytes":<Double_value>

}]}
```

stream

Stream

Stream statistics.

NAME	DESCRIPTION
streamidentifier	Statistics for identifier resource.

streamidentifier

Statistics for identifier resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the stream identifier. Minimum length = 1
pattern	<String[]>	Read-write	Values on which grouping is performed are displayed in the output as row titles. If grouping is performed on two or more fields, their values are separated by a question mark in the row title. For example, consider a selector that contains the expressions HTTP.REQ.URL and CLIENT.IP.SRC (in that order), on an appliance that has accumulated records of a number of requests for two URLs, example.com/page1.html and example.com/page2.html, from two client IP addresses,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			192.0.2.10 and 192.0.2.11. With a pattern of ? ?, the appliance performs grouping on both fields and displays statistics for the following: * Requests for example.com/abc.html from 192.0.2.10, with a row title of example.com/abc.html? 192.0.2.10. * Requests for example.com/abc.html from 192.0.2.11, with a row title of example.com/abc.html? 192.0.2.11. * Requests for example.com/def.html from 192.0.2.10, with a row title of example.com/def.html? 192.0.2.10.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			* Requests for example.com/def.html from 192.0.2.11, with a row title of example.com/def.html? 192.0.2.11. With a pattern of * ?, the appliance performs grouping on only the client IP address values and displays statistics for the following requests: * All requests from 192.0.2.10, with the IP address as the row title. * All requests from 192.0.2.11, with the IP address as the row title. With a pattern of ? *, the appliance performs grouping on only the URL values and displays statistics for the following requests:

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			* All requests for example.com/abc.html, with the URL as the row title. * All requests for example.com/def.html, with the URL as the row title. With a pattern of * *, the appliance displays one set of collective statistics for all the requests received, with no row title. With a pattern of example.com/abc.html ?, the appliance displays statistics for requests for example.com/abc.html from each unique client IP address. With a pattern of * 192.0.2.11, the appliance displays statistics for all requests from 192.0.2.11.
clearstats	<String>	Read-write	Clear the statsistics / counters.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = basic, full
sortby	<String>	Read-write	use this argument to sort by specific key. Possible values = Req, BandW, RspTime, Conn, breachcnt, pktCredits, pktsPerSecond, DroppedConns, tokens
sortorder	<String>	Read-write	use this argument to specify sort order. Default value: SORT_DESCENDING Possible values = ascending, descending
streamobjreq	<Double>	Read-only	Total number of Stream Requests recieved.
streamobjbandw	<Double>	Read-only	Total Bandwidth consumed.
streamobjresptime	<Double>	Read-only	Average response time of the stream session.
streamobjconn	<Double>	Read-only	Current connections on the stream session.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
streamobjbreachcnt	<Double>	Read-only	Total Breaching Transactions in configured interval.
streamobjpktcredits	<Double>	Read-only	Calculated Packet credits on current connection.
streamobjpktspersecond	<Double>	Read-only	Total packets recieved in configured interval.
streamobjdroppedconns	<Double>	Read-only	Total connections dropped.
streamobjtokens	<Double>	Read-only	Total LLM tokens consumed in configured interval.

Operations

(click to see Properties)

- GET (ALL)
- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/streamidentifier **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/streamidentifier? **args= name:<String_value>, pattern: <String_value> ,detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value> ,sortby: <String_value> ,sortorder: <String_value> ,sortorder: <String_value>**

Use this query-parameter to get streamidentifier resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/streamidentifier? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "streamidentifier": [ {

"name":<String_value>,

"streamobjconn":<Double_value>,

"streamobjresptime":<Double_value>,

"streamobjbreachcnt":<Double_value>,

"streamobjdroppedconns":<Double_value>,

"streamobjtokens":<Double_value>,

"streamobjpktspersecond":<Double_value>,

"streamobjpktcredits":<Double_value>,

"streamobjbandw":<Double_value>,

"streamobjreq":<Double_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/stat/streamidentifier/ name_value><String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "streamidentifier": [ {

"name":<String_value>,

"streamobjconn":<Double_value>,

"streamobjresptime":<Double_value>,

"streamobjbreachcnt":<Double_value>,

"streamobjdroppedconns":<Double_value>,

"streamobjtokens":<Double_value>,

"streamobjpktspersecond":<Double_value>,

"streamobjpktcredits":<Double_value>,

"streamobjbandw":<Double_value>,

"streamobjreq":<Double_value>

}]}
```

system

System

System statistics.

NAME	DESCRIPTION
system	Statistics for system.
systembw	Statistics for bw resource.
systemcpu	Statistics for cpu resource.

NAME	DESCRIPTION
systemmemory	Statistics for Global system memory stats resource.

system

Statistics for system.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full
voltagev12n	<Double>	Read-only	Power supply -12V output. Acceptable range is -13.20 through -10.80 volts. 9800 and 9960 platforms display standard value of -12.0V.
voltagev5n	<Double>	Read-only	Power supply -5V output. Acceptable range is -5.50 through -4.50 volts. 9800 and 9960 platforms display standard value of -5.0V.
cpuusage	<Double>	Read-only	CPU utilization percentage.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
rescpuusage	<Double>	Read-only	Shows average CPU utilization percentage if more than 1 CPU is present.
slavecpuusage	<Double>	Read-only	CPU 1 (currently the slave CPU) utilization, as percentage of capacity. Not applicable for a single-CPU system.
mastercpuusage	<Double>	Read-only	CPU 0 (currently the master CPU) utilization, as percentage of capacity.
auxvolt7	<Double>	Read-only	Voltage of a device connected to health monitoring chip through pin 7.
auxvolt6	<Double>	Read-only	Voltage of a device connected to health monitoring chip through pin 6.
auxvolt5	<Double>	Read-only	Voltage of a device connected to health monitoring chip through pin 5.
auxvolt4	<Double>	Read-only	Voltage of a device connected to health monitoring chip through pin 4.
auxvolt3	<Double>	Read-only	Voltage of a device connected to health

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			monitoring chip through pin 3.
auxvolt2	<Double>	Read-only	Voltage of a device connected to health monitoring chip through pin 2.
auxvolt1	<Double>	Read-only	Voltage of a device connected to health monitoring chip through pin 1.
auxvolt0	<Double>	Read-only	Voltage of a device connected to health monitoring chip through pin 0.
voltagevsen2	<Double>	Read-only	Voltage Sensor 2 Input. Currently only 13k Platforms will have valid value for this counter and for older platforms this will be 0.
voltagev5sb	<Double>	Read-only	Power Supply 5V Standby Voltage. Currently only 13k Platforms will have valid value for this counter and for older platforms this will be 0.
voltagevtt	<Double>	Read-only	Intel CPU Vtt power. Currently only 13k Platforms will have valid value for this counter and for older

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			platforms this will be 0.
voltagevbat	<Double>	Read-only	Onboard battery power supply output. 9800 and 9950 platforms display standard value of 5.0V.
voltagev12p	<Double>	Read-only	Power supply +12V output. Acceptable range is 10.80 through 13.20 volts.
voltagev5p	<Double>	Read-only	Power supply +5V output. Acceptable range is 4.50 through 5.50 volts.
voltagev33stby	<Double>	Read-only	Standby power supply +3.3V output. Acceptable range is 2.970 through 3.630 volts. 9800 and 9960 platforms display standard value of 3.3V. You can configure Standby 3.3V Supply Voltage by using the Set snmp alarm VOLTAGE-LOW command to set the lower limit and the Set snmp alarm VOLTAGE-HIGH command to set the upper limit.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
voltagev33main	<Double>	Read-only	Main power supply +3.3V output. Acceptable range is 2.970 through 3.630 volts. This is a critical counter. You can configure Main 3.3V Supply Voltage, by using the Set snmp alarm VOLTAGE-LOW command to set the lower limit and the Set snmp alarm VOLTAGE-HIGH command to set the upper limit.
voltagevcc1	<Double>	Read-only	CPU core 1 voltage. Acceptable range is 1.080 through 1.650 volts. If CPU 1 is not connected to the health monitoring chip, display shows voltage of CPU 0.
voltagevcc0	<Double>	Read-only	CPU core 0 voltage. Acceptable range is 1.080 through 1.650 volts.
numcpus	<Double>	Read-only	The number of CPUs on the Citrix ADC.
memusagepcnt	<Double>	Read-only	Percentage of memory utilization on Citrix ADC.
memuseinmb	<Double>	Read-only	Main memory currently in use, in megabytes.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
addimgmtcpuusagepcnt	<Double>	Read-only	Additonal Management CPU utilization percentage.
mgmtcpu0usagepcnt	<Double>	Read-only	Management CPU-0 utilization percentage.
mgmtcpuusagepcnt	<Double>	Read-only	Average Management CPU utilization percentage.
pktcpuusagepcnt	<Double>	Read-only	Average CPU utilization percentage for all packet engines excluding management PE.
cpuusagepcnt	<Double>	Read-only	CPU utilization percentage.
rescpuusagepcnt	<Double>	Read-only	Average CPU utilization percentage. Not applicable for a single-CPU system.
starttimelocal	<String>	Read-only	Time (in local timezone format) when the Citrix ADC was last started.
starttime	<String>	Read-only	Time when the Citrix ADC was last started.
disk0perusage	<Double>	Read-only	Used space in /flash partition of the disk, as a percentage.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			This is a critical counter. You can configure /flash Used (%) by using the Set snmp alarm DISK-USAGE-HIGH command.
disk1perusage	<Double>	Read-only	Used space in /var partition of the disk, as a percentage. This is a critical counter. You can configure /var Used (%) by using the Set snmp alarm DISK-USAGE-HIGH command.
cpufan0speed	<Double>	Read-only	CPU Fan 0 speed. Acceptable range is 3000 through 6000 RPM. This is a critical counter. You can configure CPU Fan 0 Speed by using the Set snmp alarm FAN-SPEED-LOW command to set the lower limit.
cpufan1speed	<Double>	Read-only	CPU Fan 1 speed. Acceptable range is 3000 through 6000 RPM. 7000 platform displays speed of CPU fan 0. This is a critical counter. You can configure CPU Fan 1 Speed by using the Set snmp

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			alarm FAN-SPEED-LOW command to set the lower limit.
systemfanspeed	<Double>	Read-only	System fan speed. Acceptable range is 3000 through 6000 RPM. This is a critical counter. You can configure System Fan Speed by using the Set snmp alarm FAN-SPEED-LOW command to set the lower limit.
fan0speed	<Double>	Read-only	System fan 1 speed. For new platforms associated pin is connected to CPU supporting fans. For platforms in which it is not connected, it will point to System Fan.
fanspeed	<Double>	Read-only	System fan 2 speed. For new platforms associated pin is connected to CPU supporting fans. For platforms in which it is not connected, it will point to System Fan
cpu0temp	<Double>	Read-only	CPU 0 temperature. 9800 and 9960 platforms display internal chip

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			temperature. This is a critical counter. You can configure CPU 0 Temperature by using the Set snmp alarm TEMPERATURE-HIGH command to set the upper limit.
cpu1temp	<Double>	Read-only	CPU 1 temperature. 9800 and 9960 platforms display internal chip temperature. 7000, 9010 and 10010 platforms display CPU 0 temperature. This is a critical counter. You can configure CPU 1 Temperature by using the Set snmp alarm TEMPERATURE-HIGH command to set the upper limit.
internaltemp	<Double>	Read-only	Internal temperature of health monitoring chip. This is a critical counter. You can configure Internal Temperature by using the Set snmp alarm TEMPERATURE-HIGH command to set the upper limit.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
powersupply1status	<String>	Read-only	Power supply 1 failure status.
powersupply2status	<String>	Read-only	Power supply 2 failure status.
powersupply3status	<String>	Read-only	Power supply 3 failure status.
powersupply4status	<String>	Read-only	Power supply 4 failure status.
disk0size	<Double>	Read-only	Size of /flash partition of the hard disk.
disk0used	<Double>	Read-only	Used space in /flash partition of the hard disk.
disk0avail	<Double>	Read-only	Available space in /flash partition of the hard disk.
disk1size	<Double>	Read-only	Size of /var partition of the hard disk.
disk1used	<Double>	Read-only	Used space in /var partition of the hard disk.
disk1avail	<Double>	Read-only	Available space in /var partition of the hard disk.
fan2speed	<Double>	Read-only	Speed of Fan 0 if associated pin is connected to health monitoring chip.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
fan3speed	<Double>	Read-only	Speed of Fan 1 if associated pin is connected to health monitoring chip.
fan4speed	<Double>	Read-only	Speed of Fan 2 if associated pin is connected to health monitoring chip.
fan5speed	<Double>	Read-only	Speed of Fan 3 if associated pin is connected to health monitoring chip.
auxtemp0	<Double>	Read-only	Temperature of a device connected to health monitoring chip through pin 0.
auxtemp1	<Double>	Read-only	Temperature of a device connected to health monitoring chip through pin 1.
auxtemp2	<Double>	Read-only	Temperature of a device connected to health monitoring chip through pin 2.
auxtemp3	<Double>	Read-only	Temperature of a device connected to health monitoring chip through pin 3.
timesincestart	<String>	Read-only	Seconds since the Citrix ADC started.
memsizemb	<Double>	Read-only	Total amount of system memory, in megabytes.

Operations

(click to see Properties)

- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/system **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/system? **args=detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get system resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/system? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "system": [ {

"cpufan1speed":<Double_value>,

"auxtemp2":<Double_value>,

"voltagevcc0":<Double_value>,

"memusagepcnt":<Double_value>,

"fan2speed":<Double_value>,

"voltagevbat":<Double_value>,

"auxtemp0":<Double_value>,

"auxvolt3":<Double_value>,

"timesincestart":<String_value>,

"systemfanspeed":<Double_value>,

"disk1used":<Double_value>,
```

```
"pktcpuusagepcnt":<Double_value>,

"cpu0temp":<Double_value>,

"voltagev33stby":<Double_value>,

"rescpuusagepcnt":<Double_value>,

"disk0perusage":<Double_value>,

"addimgmtcpuusagepcnt":<Double_value>,

"auxvolt1":<Double_value>,

"voltagev5sb":<Double_value>,

"fan4speed":<Double_value>,

"auxvolt4":<Double_value>,

"disk1avail":<Double_value>,

"auxvolt6":<Double_value>,

"memsizemb":<Double_value>,

"cpu1temp":<Double_value>,

"cpuusage":<Double_value>,

"mastercpuusage":<Double_value>,

"disk0size":<Double_value>,

"starttime":<String_value>,

"auxvolt7":<Double_value>,

"powersupply3status":<String_value>,

"cpuusagepcnt":<Double_value>,

"auxvolt5":<Double_value>,
```

```
"fan3speed":<Double_value>,

"mgmtcpuusagepcnt":<Double_value>,

"memuseinmb":<Double_value>,

"disk1size":<Double_value>,

"fan0speed":<Double_value>,

"voltagev33main":<Double_value>,

"voltagev12n":<Double_value>,

"rescpuusage":<Double_value>,

"voltagev5n":<Double_value>,

"voltagevcc1":<Double_value>,

"disk1perusage":<Double_value>,

"starttimelocal":<String_value>,

"mgmtcpu0usagepcnt":<Double_value>,

"powersupply2status":<String_value>,

"slavecpuusage":<Double_value>,

"voltagev12p":<Double_value>,

"disk0avail":<Double_value>,

"auxtemp1":<Double_value>,

"internaltemp":<Double_value>,

"voltagev5p":<Double_value>,

"disk0used":<Double_value>,

"cpufan0speed":<Double_value>,
```

```
"voltagevsen2":<Double_value>,

"numcpus":<Double_value>,

"fan5speed":<Double_value>,

"powersupply4status":<String_value>,

"fanspeed":<Double_value>,

"voltagevtt":<Double_value>,

"auxvolt0":<Double_value>,

"auxtemp3":<Double_value>,

"powersupply1status":<String_value>,

"auxvolt2":<Double_value>

}]}
```

systembw

Statistics for bw resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full
httpcltpoolinactive	<Double>	Read-only	No of requests sent from BW client.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
httpcltpooloutactive	<Double>	Read-only	No of responses Received.
httpsvr200okresp	<Double>	Read-only	Number of 200 Ok response sent from the BW appliance.
httpsvr200okresprate	<Double>	Read-only	Rate (/s) counter for httpsvr200okresp
httpsvr404notfound	<Double>	Read-only	Number of 404 Not Found responses sent
httpsvr404notfoundrate	<Double>	Read-only	Rate (/s) counter for httpsvr404notfound
httpclterrstray	<Double>	Read-only	Number of stray packets received from server without HTTP request
httpclterrstrayrate	<Double>	Read-only	Rate (/s) counter for httpclterrstray
httpclttfplwm	<Double>	Read-only	Number of Responses Falling on LWM for TTFP.
httpclttfplwmrate	<Double>	Read-only	Rate (/s) counter for httpclttfplwm
httpclttfp_0	<Double>	Read-only	Number of Responses Falling on Band-0 for TTFP.
httpclttfp_0rate	<Double>	Read-only	Rate (/s) counter for httpclttfp_0

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
httpcltttfp_1	<Double>	Read-only	Number of Responses Falling on Band-1 for TTFP.
httpcltttfp_1rate	<Double>	Read-only	Rate (/s) counter for httpcltttfp_1
httpcltttfp_2	<Double>	Read-only	Number of Responses Falling on Band-2 for TTFP.
httpcltttfp_2rate	<Double>	Read-only	Rate (/s) counter for httpcltttfp_2
httpcltttfp_3	<Double>	Read-only	Number of Responses Falling on Band-3 for TTFP.
httpcltttfp_3rate	<Double>	Read-only	Rate (/s) counter for httpcltttfp_3
httpcltttfp_4	<Double>	Read-only	Number of Responses Falling on Band-4 for TTFP.
httpcltttfp_4rate	<Double>	Read-only	Rate (/s) counter for httpcltttfp_4
httpcltttfp_5	<Double>	Read-only	Number of Responses Falling on Band-5 for TTFP.
httpcltttfp_5rate	<Double>	Read-only	Rate (/s) counter for httpcltttfp_5
httpcltttfp_6	<Double>	Read-only	Number of Responses Falling on Band-6 for TTFP.
httpcltttfp_6rate	<Double>	Read-only	Rate (/s) counter for httpcltttfp_6

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
httpclttfp_7	<Double>	Read-only	Number of Responses Falling on Band-7 for TTFP.
httpclttfp_7rate	<Double>	Read-only	Rate (/s) counter for httpclttfp_7
httpclttfphwm	<Double>	Read-only	Number of Responses Falling on HWM for TTFP.
httpclttfphwmrate	<Double>	Read-only	Rate (/s) counter for httpclttfphwm
httpclttfpmax	<Double>	Read-only	Peak RTT observed for Time to First response packet.
httpclttlplwm	<Double>	Read-only	Number of Responses Falling on LWM for TTLP.
httpclttlplwmrate	<Double>	Read-only	Rate (/s) counter for httpclttlplwm
httpclttlp_0	<Double>	Read-only	Number of Responses Falling on Band-0 for TTLP.
httpclttlp_0rate	<Double>	Read-only	Rate (/s) counter for httpclttlp_0
httpclttlp_1	<Double>	Read-only	Number of Responses Falling on Band-1 for TTLP.
httpclttlp_1rate	<Double>	Read-only	Rate (/s) counter for httpclttlp_1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
httpclttlp_2	<Double>	Read-only	Number of Responses Falling on Band-2 for TTLP.
httpclttlp_2rate	<Double>	Read-only	Rate (/s) counter for httpclttlp_2
httpclttlp_3	<Double>	Read-only	Number of Responses Falling on Band-3 for TTLP.
httpclttlp_3rate	<Double>	Read-only	Rate (/s) counter for httpclttlp_3
httpclttlp_4	<Double>	Read-only	Number of Responses Falling on Band-4 for TTLP.
httpclttlp_4rate	<Double>	Read-only	Rate (/s) counter for httpclttlp_4
httpclttlp_5	<Double>	Read-only	Number of Responses Falling on Band-5 for TTLP.
httpclttlp_5rate	<Double>	Read-only	Rate (/s) counter for httpclttlp_5
httpclttlp_6	<Double>	Read-only	Number of Responses Falling on Band-6 for TTLP.
httpclttlp_6rate	<Double>	Read-only	Rate (/s) counter for httpclttlp_6
httpclttlp_7	<Double>	Read-only	Number of Responses Falling on Band-7 for TTLP.
httpclttlp_7rate	<Double>	Read-only	Rate (/s) counter for httpclttlp_7

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
httpclttlphwm	<Double>	Read-only	Number of Responses Falling on HWM for TTLP.
httpclttlphwmrate	<Double>	Read-only	Rate (/s) counter for httpclttlphwm
httpclttlpmax	<Double>	Read-only	Peak RTT observed for Time to Last response packet.

Operations

(click to see Properties)

- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/systembw **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/systembw? **args=detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get systembw resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/systembw? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "systembw": [ {

"httpclttlphwmrate":<Double_value>,

"httpclttfp_0rate":<Double_value>,

"httpclttfp_3":<Double_value>,

"httpclttfp_7":<Double_value>,
```

```
"httpclttlp_3rate":<Double_value>,

"httpclttlp_0":<Double_value>,

"httpclttlp_7rate":<Double_value>,

"httpclttfp_5rate":<Double_value>,

"httpsvr404notfound":<Double_value>,

"httpclttlp_5":<Double_value>,

"httpclttfplwmrate":<Double_value>,

"httpclttfphwm":<Double_value>,

"httpclttlp_4":<Double_value>,

"httpclttfp_4rate":<Double_value>,

"httpclttlp_6rate":<Double_value>,

"httpclttfp_2rate":<Double_value>,

"httpclttlpmax":<Double_value>,

"httpclttlp_1rate":<Double_value>,

"httpclterrstrayrate":<Double_value>,

"httpsvr200okresprate":<Double_value>,

"httpclttfp_6":<Double_value>,

"httpclttfp_1":<Double_value>,

"httpclttlp_2":<Double_value>,

"httpsvr200okresp":<Double_value>,

"httpclttlplwm":<Double_value>,

"httpclttlp_1":<Double_value>,
```

```
"httpclttfp_2":<Double_value>,

"httpclttlp_6":<Double_value>,

"httpclttfplwm":<Double_value>,

"httpclttlp_2rate":<Double_value>,

"httpclttfp_1rate":<Double_value>,

"httpclttfpmax":<Double_value>,

"httpclttfp_6rate":<Double_value>,

"httpcltpooloutactive":<Double_value>,

"httpcltpoolinactive":<Double_value>,

"httpclttlp_4rate":<Double_value>,

"httpclterrstray":<Double_value>,

"httpclttlphwm":<Double_value>,

"httpclttfp_4":<Double_value>,

"httpclttlplwmrate":<Double_value>,

"httpclttfp_5":<Double_value>,

"httpclttlp_5rate":<Double_value>,

"httpclttfp_3rate":<Double_value>,

"httpclttfp_0":<Double_value>,

"httpclttfp_7rate":<Double_value>,

"httpclttlp_0rate":<Double_value>,

"httpsvr404notfoundrate":<Double_value>,

"httpclttlp_3":<Double_value>,
```

```
"httpclttfphwmrate":<Double_value>,

"httpclttlp_7":<Double_value>

}]}
```

systemcpu

Statistics for cpu resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
id	<Integer>	Read-write	ID of the CPU for which to display statistics. Default value: 65535 Minimum value = 0 Maximum value = 65534
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full
percpuuse	<Double>	Read-only	CPU utilization percentage.

Operations

(click to see Properties)

- GET (ALL)
- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/systemcpu **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/systemcpu? **args=id: <Integer_value> ,detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get systemcpu resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/systemcpu? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "systemcpu": [ {

"id":<Integer_value>,

"percpuuse":<Double_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/stat/systemcpu/ id_value><Integer> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "systemcpu": [ {

"id":<Integer_value>,

"percpuuse":<Double_value>

}]}
```

systemmemory

Statistics for Global system memory stats resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full
cacmemmaxmemlimitpcnt	<Double>	Read-only	Integrated Cache memory in use percent.
cacmemmaxmemlimit	<Double>	Read-only	Integrated Cache memory in use, in megabytes.
shmemerrallocfailed	<Double>	Read-only	Total shared memory allocation failed.
shmemallocpcnt	<Double>	Read-only	Shared memory in use percent.
shmemallocinmb	<Double>	Read-only	Shared memory in use, in megabytes.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
shmemtotinmb	<Double>	Read-only	Total shared memory allowed to allocate, in megabytes.
memtotallocfailed	<Double>	Read-only	Total system memory allocation failed.
memtotfree	<Double>	Read-only	Total Free PE Memory in the System.
memusagepcnt	<Double>	Read-only	Percentage of memory utilization on Citrix ADC.
memtotuseinmb	<Double>	Read-only	Total Citrix ADC Memory in use, in megabytes.
memtotallocpcnt	<Double>	Read-only	Currently allocated memory in percent.
memtotallocmb	<Double>	Read-only	Currently allocated memory, in megabytes.
memtotinmb	<Double>	Read-only	Total memory available (grabbed) for use by packet engine (PE), in megabytes.
memtotavail	<Double>	Read-only	Total system memory available for PE to grab from the system.
cacmemmaxsyslimitmb	<Double>	Read-only	Integrated Cache memory, in megabytes.

Operations

(click to see Properties)

- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/systemmemory **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/systemmemory? **args=detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get systemmemory resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/systemmemory? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "systemmemory": [ {

"memtotuseinmb":<Double_value>,

"shmemerrallocfailed":<Double_value>,

"memusagepcnt":<Double_value>,

"cacmemmaxmemlimit":<Double_value>,

"shmemallocpcnt":<Double_value>,

"memtotinmb":<Double_value>,

"shmemtotinmb":<Double_value>,

"memtotavail":<Double_value>,

"shmemallocinmb":<Double_value>,

"cacmemmaxmemlimitpcnt":<Double_value>,

"memtotallocfailed":<Double_value>,
```

```
"memtotallocpcnt":<Double_value>,

"cacmemmaxsyslimitmb":<Double_value>,

"memtotallocmb":<Double_value>,

"memtotfree":<Double_value>

}]}
```

tm

Traffic Management

TM session/policy statistics.

NAME	DESCRIPTION
tmsessionpolicy	Statistics for TM session policy resource.
tmtrafficpolicy	Statistics for TM traffic policy resource.

tmsessionpolicy

Statistics for TM session policy resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the advanced tmsession policy for which to display statistics. If no name is specified, statistics for all advanced tmsession polices are shown.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum length = 1
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full
pipolicyhits	<Double>	Read-only	Number of hits on the policy
pipolicyhitsrate	<Double>	Read-only	Rate (/s) counter for pipolicyhits
pipolicyundefhits	<Double>	Read-only	Number of undef hits on the policy
pipolicyundefhitsrate	<Double>	Read-only	Rate (/s) counter for pipolicyundefhits

Operations

(click to see Properties)

- GET (ALL)
- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/tmsessionpolicy **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/tmsessionpolicy? **args=name: <String_value> ,detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get tmsessionpolicy resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/tmsessionpolicy? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "tmsessionpolicy": [ {

"name":<String_value>,

"pipolicyundefhitsrate":<Double_value>,

"pipolicyhitsrate":<Double_value>,

"pipolicyundefhits":<Double_value>,

"pipolicyhits":<Double_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/stat/tmsessionpolicy/ name_value><String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "tmsessionpolicy": [ {

"name":<String_value>,

"pipolicyundefhitsrate":<Double_value>,

"pipolicyhitsrate":<Double_value>,
```

```
"pipolicyundefhits":<Double_value>,

"pipolicyhits":<Double_value>

}]}
```

tmtrafficpolicy

Statistics for TM traffic policy resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	The name of the TM traffic policy for which statistics will be displayed. If not given statistics are shown for all policies. Minimum length = 1
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full
pipolicyhits	<Double>	Read-only	Number of hits on the policy
pipolicyhitsrate	<Double>	Read-only	Rate (/s) counter for pipolicyhits

Operations

(click to see Properties)

- GET (ALL)
- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/tmtrafficpolicy **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/tmtrafficpolicy? **args=name: <String_value> ,detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get tmtrafficpolicy resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/tmtrafficpolicy? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "tmtrafficpolicy": [ {

"name":<String_value>,

"pipolicyhits":<Double_value>,

"pipolicyhitsrate":<Double_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/stat/tmtrafficpolicy/ name_value><String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "tmtrafficpolicy": [ {

"name":<String_value>,

"pipolicyhits":<Double_value>,

"pipolicyhitsrate":<Double_value>

}]}
```

transform

Transform

URL Transformation statistics.

NAME	DESCRIPTION
transformpolicy	Statistics for URL Transformation policy resource.
transformpolicylabel	Statistics for transform policy label resource.

transformpolicy

Statistics for URL Transformation policy resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the policy. Minimum length = 1
clearstats	<String>	Read-write	Clear the statsistics / counters.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = basic, full
pipolicyhits	<Double>	Read-only	Number of hits on the policy
pipolicyhitsrate	<Double>	Read-only	Rate (/s) counter for pipolicyhits
pipolicyundefhits	<Double>	Read-only	Number of undef hits on the policy
pipolicyundefhitsrate	<Double>	Read-only	Rate (/s) counter for pipolicyundefhits

Operations

(click to see Properties)

- GET (ALL)
- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/transformpolicy **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/transformpolicy? **args=name: <String_value> ,detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get transformpolicy resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/transformpolicy? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "transformpolicy": [ {

"name":<String_value>,

"pipolicyundefhitsrate":<Double_value>,
```

```
"pipolicyhitsrate":<Double_value>,

"pipolicyundefhits":<Double_value>,

"pipolicyhits":<Double_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/stat/transformpolicy/ name_value><String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "transformpolicy": [ {

"name":<String_value>,

"pipolicyundefhitsrate":<Double_value>,

"pipolicyhitsrate":<Double_value>,

"pipolicyundefhits":<Double_value>,

"pipolicyhits":<Double_value>

}]}
```

transformpolicylabel

Statistics for transform policy label resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
labelname	<String>	Read-write	The name of the URL Transformation policy label. Minimum length = 1
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full
pipolicylabelhits	<Double>	Read-only	Number of times policy label was invoked.
pipolicylabelhitsrate	<Double>	Read-only	Rate (/s) counter for pipolicylabelhits

Operations

(click to see Properties)

- GET (ALL)
- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/transformpolicylabel **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/transformpolicylabel? **args=labelname: <String_value> ,detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get transformpolicylabel resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/transformpolicylabel? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "transformpolicylabel": [ {

"labelname":<String_value>,

"pipolicylabelhits":<Double_value>,

"pipolicylabelhitsrate":<Double_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/stat/transformpolicylabel/ labelname_value><String>
HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "transformpolicylabel": [ {

"labelname":<String_value>,

"pipolicylabelhits":<Double_value>,

"pipolicylabelhitsrate":<Double_value>

}]}
```

tunnel

Tunnel

SSL VPN Tunnel statistics.

NAME	DESCRIPTION
tunneltrafficpolicy	Statistics for tunnel policy resource.

tunneltrafficpolicy

Statistics for tunnel policy resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the advanced tunnel traffic policy. Minimum length = 1
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
pipolicyhits	<Double>	Read-only	Number of hits on the policy
pipolicyhitsrate	<Double>	Read-only	Rate (/s) counter for pipolicyhits
pipolicyundefhits	<Double>	Read-only	Number of undef hits on the policy
pipolicyundefhitsrate	<Double>	Read-only	Rate (/s) counter for pipolicyundefhits

Operations

(click to see Properties)

- GET (ALL)
- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/tunneltrafficpolicy **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/tunneltrafficpolicy? **args=name: <String_value> ,detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get tunneltrafficpolicy resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/tunneltrafficpolicy? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "tunneltrafficpolicy": [ {

"name":<String_value>,

"pipolicyundefhitsrate":<Double_value>,

"pipolicyhitsrate":<Double_value>,
```

```
"pipolicyundefhits":<Double_value>,

"pipolicyhits":<Double_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/stat/tunneltrafficpolicy/ name_value><String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "tunneltrafficpolicy": [ {

"name":<String_value>,

"pipolicyundefhitsrate":<Double_value>,

"pipolicyhitsrate":<Double_value>,

"pipolicyundefhits":<Double_value>,

"pipolicyhits":<Double_value>

}]}
```

user

User

User protocol statistics.

NAME	DESCRIPTION
uservserver	Statistics for virtual server resource.

uservserver

Statistics for virtual server resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the user defined virtual server. If no name is provided, statistical data of all configured user defined virtual servers is displayed. Minimum length = 1
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full
sortby	<String>	Read-write	use this argument to sort by specific key. Possible values = Hits

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
sortorder	<String>	Read-write	use this argument to specify sort order. Default value: SORT_DESCENDING Possible values = ascending, descending
establishedconn	<Double>	Read-only	Number of client connections in ESTABLISHED state.
inactsvcs	<Double>	Read-only	number of INACTIVE services bound to a vserver
vslbhealth	<Double>	Read-only	Health of the vserver. This gives percentage of UP services bound to this vserver.
primaryipaddress	<String>	Read-only	IP address of the vserver
primaryport	<Integer>	Read-only	The port on which the service is running.
protocolname	<String>	Read-only	Protocol associated with the vserver
state	<String>	Read-only	Current state of the server. There are seven possible values: UP(7), DOWN(1), UNKNOWN(2),

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			BUSY(3), OFS(Out of Service)(4), TROFS(Transition Out of Service)(5), TROFS_DOWN(Down When going Out of Service)(8)
actsvcs	<Double>	Read-only	number of ACTIVE services bound to a vserver
tothits	<Double>	Read-only	Total vserver hits
hitsrate	<Double>	Read-only	Rate (/s) counter for tothits
totalrequests	<Double>	Read-only	Total number of requests received on this service or virtual server. (This applies to HTTP/SSL services and servers.)
requestsrate	<Double>	Read-only	Rate (/s) counter for totalrequests
totalresponses	<Double>	Read-only	Number of responses received on this service or virtual server. (This applies to HTTP/SSL services and servers.)
responsesrate	<Double>	Read-only	Rate (/s) counter for totalresponses
totalrequestbytes	<Double>	Read-only	Total number of request bytes received on this

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			service or virtual server.
requestbytesrate	<Double>	Read-only	Rate (/s) counter for totalrequestbytes
totalresponsebytes	<Double>	Read-only	Number of response bytes received by this service or virtual server.
responsebytesrate	<Double>	Read-only	Rate (/s) counter for totalresponsebytes
totalpktsrecvd	<Double>	Read-only	Total number of packets received by this service or virtual server.
pktsrecvdrate	<Double>	Read-only	Rate (/s) counter for totalpktsrecvd
totalpktssent	<Double>	Read-only	Total number of packets sent.
pktssentrate	<Double>	Read-only	Rate (/s) counter for totalpktssent
curclntconnections	<Double>	Read-only	Number of current client connections.
cursrvrconnections	<Double>	Read-only	Number of current connections to the actual servers behind the virtual server.
invalidrequestrespon se	<Double>	Read-only	Number invalid requests/responses on this vserver

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
invalidrequestrespon sedropped	<Double>	Read-only	Number invalid requests/responses dropped on this vserver

Operations

(click to see Properties)

- GET (ALL)
- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/uservserver **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/uservserver? **args=name: <String_value> ,detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value> ,sortby: <String_value> ,sortorder: <String_value> ,sortorder: <String_value>**

Use this query-parameter to get uservserver resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/uservserver? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "uservserver": [ {

"name":<String_value>,

"totalresponsebytes":<Double_value>,

"hitsrate":<Double_value>,

"requestbytesrate":<Double_value>,

"totalresponses":<Double_value>,
```

```
"establishedconn":<Double_value>,

"actsvcs":<Double_value>,

"protocolname":<String_value>,

"primaryport":<Integer_value>,

"totalrequestbytes":<Double_value>,

"tothits":<Double_value>,

"vslbhealth":<Double_value>,

"responsesrate":<Double_value>,

"totalpktsrecvd":<Double_value>,

"invalidrequestresponsedropped":<Double_value>,

"cursrvrconnections":<Double_value>,

"pktsrecvdrate":<Double_value>,

"inactsvcs":<Double_value>,

"primaryipaddress":<String_value>,

"state":<String_value>,

"responsebytesrate":<Double_value>,

"curclntconnections":<Double_value>,

"totalpktssent":<Double_value>,

"requestsrate":<Double_value>,

"invalidrequestresponse":<Double_value>,

"pktssentrate":<Double_value>,

"totalrequests":<Double_value>
```

```
}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/stat/uservserver/ name_value><String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "uservserver": [ {

"name":<String_value>,

"totalresponsebytes":<Double_value>,

"hitsrate":<Double_value>,

"requestbytesrate":<Double_value>,

"totalresponses":<Double_value>,

"establishedconn":<Double_value>,

"actsvcs":<Double_value>,

"protocolname":<String_value>,

"primaryport":<Integer_value>,
```

```
"totalrequestbytes":<Double_value>,

"tothits":<Double_value>,

"vslbhealth":<Double_value>,

"responsesrate":<Double_value>,

"totalpktsrecvd":<Double_value>,

"invalidrequestresponsedropped":<Double_value>,

"cursrvrconnections":<Double_value>,

"pktsrecvdrate":<Double_value>,

"inactsvcs":<Double_value>,

"primaryipaddress":<String_value>,

"state":<String_value>,

"responsebytesrate":<Double_value>,

"curclntconnections":<Double_value>,

"totalpktssent":<Double_value>,

"requestsrate":<Double_value>,

"invalidrequestresponse":<Double_value>,

"pktssentrate":<Double_value>,

"totalrequests":<Double_value>

}]}
```

videooptimization

VideoOptimization

Video optimization feature is used to show (i) the stats of different media types that are being served by the Citrix ADC and (ii) the details of optimization applied on ABR videos

NAME	DESCRIPTION
videooptimization	Statistics for videooptimization.
videooptimizationdetectionpolicy	Statistics for videooptimization detectionpolicy resource.
videooptimizationdetectionpolicylabel	Statistics for videooptimization detection policy label resource.
videooptimizationpacingpolicy	Statistics for videooptimization pacingpolicy resource.
videooptimizationpacingpolicylabel	Statistics for videooptimization pacing policy label resource.

videooptimization

Statistics for videooptimization.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
voctpdvideo	<Double>	Read-only	Total number of progressive download HTTP videos
voctpdvideorate	<Double>	Read-only	Rate (/s) counter for voctpdvideo
voctabvideo	<Double>	Read-only	Total number of adaptive bitrate HTTP videos
voctabvideorate	<Double>	Read-only	Rate (/s) counter for voctabvideo
voeabvideo	<Double>	Read-only	Total number of adaptive bitrate HTTPS videos
voeabvideorate	<Double>	Read-only	Rate (/s) counter for voeabvideo
voquicvideo	<Double>	Read-only	Total number of QUIC videos
voquicvideorate	<Double>	Read-only	Rate (/s) counter for voquicvideo
vovideooptother	<Double>	Read-only	Non video traffic
vovideoopherrate	<Double>	Read-only	Rate (/s) counter for vovideooptother
voctabvideoses	<Double>	Read-only	Total number of adaptive bitrate HTTP video sessions
voctabvideosesrate	<Double>	Read-only	Rate (/s) counter for voctabvideoses

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
voeabvideoses	<Double>	Read-only	Total number of adaptive bitrate HTTPS videos
voeabvideosesrate	<Double>	Read-only	Rate (/s) counter for voeabvideoses
voquicvideoses	<Double>	Read-only	Total number of sessions with QUIC videos
voquicvideosesrate	<Double>	Read-only	Rate (/s) counter for voquicvideoses
voctpdvideobytes	<Double>	Read-only	Total number of bytes for progressive download HTTP videos
voctpdvideobytesrate	<Double>	Read-only	Rate (/s) counter for voctpdvideobytes
voctabvideobytes	<Double>	Read-only	Total number of bytes for adaptive bitrate HTTP videos
voctabvideobytesrate	<Double>	Read-only	Rate (/s) counter for voctabvideobytes
voeabvideobytes	<Double>	Read-only	Total number of bytes for adaptive bitrate HTTPS videos
voeabvideobytesrate	<Double>	Read-only	Rate (/s) counter for voeabvideobytes
voquicvideobytes	<Double>	Read-only	Total number of bytes for QUIC videos

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
voquicvideobytesrate	<Double>	Read-only	Rate (/s) counter for voquicvideobytes
vovideooptotherbytes	<Double>	Read-only	Total number of bytes for non video traffic
vovideoopherbytesrate	<Double>	Read-only	Rate (/s) counter for vovideooptotherbytes

Operations

(click to see Properties)

- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/videooptimization **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/videooptimization? **args=detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get videooptimization resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/videooptimization? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "videooptimization": [ {

"vovideoopherbytesrate":<Double_value>,

"vovideooptotherbytes":<Double_value>,

"voeabvideo":<Double_value>,

"voctabvideosesrate":<Double_value>,
```

```
"vovideoopherrate":<Double_value>,

"voeabvideorate":<Double_value>,

"voquicvideosesrate":<Double_value>,

"voeabvideosesrate":<Double_value>,

"voeabvideobytes":<Double_value>,

"voctabvideo":<Double_value>,

"voquicvideorate":<Double_value>,

"voquicvideobytesrate":<Double_value>,

"voctabvideoses":<Double_value>,

"voeabvideobytesrate":<Double_value>,

"voquicvideobytes":<Double_value>,

"vovideooptother":<Double_value>,

"voctpdvideo":<Double_value>,

"voeabvideoses":<Double_value>,

"voctpdvideorate":<Double_value>,

"voctpdvideobytesrate":<Double_value>,

"voctpdvideobytes":<Double_value>,

"voctabvideorate":<Double_value>,

"voquicvideo":<Double_value>,

"voctabvideobytes":<Double_value>,

"voquicvideoses":<Double_value>,

"voctabvideobytesrate":<Double_value>
```

```
}]}
```

videooptimizationdetectionpolicy

Statistics for videooptimization detectionpolicy resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the Video Optimization detection policy for which to show detailed statistics. Minimum length = 1
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full
pipolicyhits	<Double>	Read-only	Number of hits on the policy
pipolicyhitsrate	<Double>	Read-only	Rate (/s) counter for pipolicyhits
pipolicyundefhits	<Double>	Read-only	Number of undef hits on the policy
pipolicyundefhitsrate	<Double>	Read-only	Rate (/s) counter for pipolicyundefhits

Operations

(click to see Properties)

- GET (ALL)
- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/videooptimizationdetectionpolicy **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/videooptimizationdetectionpolicy? **args=name: <String_value> ,detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get videooptimizationdetectionpolicy resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/videooptimizationdetectionpolicy? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "videooptimizationdetectionpolicy": [ {

"name":<String_value>,

"pipolicyundefhits":<Double_value>,

"pipolicyhits":<Double_value>,

"pipolicyundefhitsrate":<Double_value>,

"pipolicyhitsrate":<Double_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/stat/videooptimizationdetectionpolicy/ name_value><String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "videooptimizationdetectionpolicy": [ {

"name":<String_value>,

"pipolicyundefhits":<Double_value>,

"pipolicyhits":<Double_value>,

"pipolicyundefhitsrate":<Double_value>,

"pipolicyhitsrate":<Double_value>

}]}
```

videooptimizationdetectionpolicylabel

Statistics for videooptimization detection policy label resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
labelname	<String>	Read-write	Name of the videooptimization detection policy label. Minimum length = 1
clearstats	<String>	Read-write	Clear the statsistics / counters.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = basic, full
pipolicylabelhits	<Double>	Read-only	Number of times policy label was invoked.
pipolicylabelhitsrate	<Double>	Read-only	Rate (/s) counter for pipolicylabelhits

Operations

(click to see Properties)

- GET (ALL)
- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/videooptimizationdetectionpolicylabel **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/videooptimizationdetectionpolicylabel? **args=labelname: <String_value> ,detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get videooptimizationdetectionpolicylabel resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/videooptimizationdetectionpolicylabel? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "videooptimizationdetectionpolicylabel": [ {

"labelname":<String_value>,

"pipolicylabelhits":<Double_value>,
```

```
"pipolicylabelhitsrate":<Double_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/stat/videooptimizationdetectionpolicylabel/ labelname_value><String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "videooptimizationdetectionpolicylabel": [ {

"labelname":<String_value>,

"pipolicylabelhits":<Double_value>,

"pipolicylabelhitsrate":<Double_value>

}]}
```

videooptimizationpacingpolicy

Statistics for videooptimization pacingpolicy resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the Video Optimization Pacing policy for which to show detailed statistics. Minimum length = 1
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full
pipolicyhits	<Double>	Read-only	Number of hits on the policy
pipolicyhitsrate	<Double>	Read-only	Rate (/s) counter for pipolicyhits
pipolicyundefhits	<Double>	Read-only	Number of undef hits on the policy
pipolicyundefhitsrate	<Double>	Read-only	Rate (/s) counter for pipolicyundefhits

Operations

(click to see Properties)

- GET (ALL)
- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/videooptimizationpacingpolicy **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/videooptimizationpacingpolicy? **args=name: <String_value> ,detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get videooptimizationpacingpolicy resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/videooptimizationpacingpolicy? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "videooptimizationpacingpolicy": [ {

"name":<String_value>,

"pipolicyhitsrate":<Double_value>,

"pipolicyundefhitsrate":<Double_value>,

"pipolicyhits":<Double_value>,

"pipolicyundefhits":<Double_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/stat/videooptimizationpacingpolicy/ name_value><String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "videooptimizationpacingpolicy": [ {

"name":<String_value>,

"pipolicyhitsrate":<Double_value>,

"pipolicyundefhitsrate":<Double_value>,

"pipolicyhits":<Double_value>,

"pipolicyundefhits":<Double_value>

}]}
```

videooptimizationpacingpolicylabel

Statistics for videooptimization pacing policy label resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
labelname	<String>	Read-write	Name of the videooptimization pacing policy label. Minimum length = 1
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full
pipolicylabelhits	<Double>	Read-only	Number of times policy label was invoked.
pipolicylabelhitsrate	<Double>	Read-only	Rate (/s) counter for pipolicylabelhits

Operations

(click to see Properties)

- GET (ALL)
- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/videooptimizationpacingpolicylabel **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/videooptimizationpacingpolicylabel?**args=labelname: <String_value> ,detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get videooptimizationpacingpolicylabel resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/videooptimizationpacingpolicylabel? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "videooptimizationpacingpolicylabel": [ {

"labelname":<String_value>,

"pipolicylabelhits":<Double_value>,

"pipolicylabelhitsrate":<Double_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/stat/videooptimizationpacingpolicylabel/ labelname_value><String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "videooptimizationpacingpolicylabel": [ {

"labelname":<String_value>,

"pipolicylabelhits":<Double_value>,

"pipolicylabelhitsrate":<Double_value>

}]}
```

vpn

SSL VPN

Virtual Private Network statistics.

NAME	DESCRIPTION
vpn	Statistics for vpn.
vpnurlpolicy	Statistics for VPN url policy resource.
vpnvserver	Statistics for VPN virtual server resource.

vpn

Statistics for vpn.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full
indexhtmlhit	<Double>	Read-only	Number of requests for VPN login page.
indexhtmlnoserved	<Double>	Read-only	Number of failures to display VPN login page.
cfghtmlserved	<Double>	Read-only	Number of client configuration requests received by VPN server.
cfghtmlservedrate	<Double>	Read-only	Rate (/s) counter for cfghtmlserved
dnsreqhit	<Double>	Read-only	Number of DNS queries resolved by VPN server.
dnsreqhitrate	<Double>	Read-only	Rate (/s) counter for dnsreqhit
winsrequesthit	<Double>	Read-only	Number of WINS queries resolved by VPN server.
winsrequesthitrate	<Double>	Read-only	Rate (/s) counter for winsrequesthit

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
csrequesthit	<Double>	Read-only	Number of SSL VPN tunnels formed between VPN server and client.
csrequesthitrate	<Double>	Read-only	Rate (/s) counter for csrequesthit
csnonhttpprobehit	<Double>	Read-only	Number of probes from VPN to back-end non-HTTP servers that have been accessed by the VPN client.
csnonhttpprobehitrate	<Double>	Read-only	Rate (/s) counter for csnonhttpprobehit
cshttpprobehit	<Double>	Read-only	Number of probes from VPN to back-end HTTP servers that have been accessed by the VPN client.
cshttpprobehitrate	<Double>	Read-only	Rate (/s) counter for cshttpprobehit
totalcsconnsucc	<Double>	Read-only	Number of successful probes to all back-end servers.
csconnsuccrate	<Double>	Read-only	Rate (/s) counter for totalcsconnsucc
totalfsrequest	<Double>	Read-only	Number of file system requests received by VPN server.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
fsrequestrate	<Double>	Read-only	Rate (/s) counter for totalfsrequest
vpnlicensefail	<Double>	Read-only	Number of users not able to login because of license unavailability.
svpnhttpdtotalrequests	<Double>	Read-only	Total number of requests from VPN to Apache
svpnhttpdtotalresponses	<Double>	Read-only	Total number of responses from Apache for VPN
svpnhttpdtotalrequestscachehits	<Double>	Read-only	Total number of vpn requests to Apache hitting cache
svpnhttpdcurserverconnectionsopen	<Double>	Read-only	Number of current VPN to Apache open server connections
svpnreqwaftotblock	<Double>	Read-only	Total Number of requests that are blocked as part of Appfw Validation for VPN
iipdisabledmipused	<Double>	Read-only	Number of times SNIP is used as IIP is disabled.
iipdisabledmipusedrate	<Double>	Read-only	Rate (/s) counter for iipdisabledmipused
iipfailedmipused	<Double>	Read-only	Number of times SNIP is used as IIP assignment failed.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
iipfailedmipusedrate	<Double>	Read-only	Rate (/s) counter for iipfailedmipused
iipspillovermipused	<Double>	Read-only	Number of times SNIP is used on IIP Spillover.
iipspillovermipusedrate	<Double>	Read-only	Rate (/s) counter for iipspillovermipused
iipdisabledmipdisabled	<Double>	Read-only	Both IIP and SNIP is disabled.
iipdisabledmipdisabledrate	<Double>	Read-only	Rate (/s) counter for iipdisabledmipdisabled
iipfailedmipdisabled	<Double>	Read-only	Number of times IIP assignment failed and SNIP is disabled.
iipfailedmipdisabledrate	<Double>	Read-only	Rate (/s) counter for iipfailedmipdisabled
csgtotalconnectedusers	<Double>	Read-only	Number of total users connected across VPN vservers
csgconnectedusersrate	<Double>	Read-only	Rate (/s) counter for csgtotalconnectedusers
socksmethreqrcvd	<Double>	Read-only	Number of received SOCKS method request.
socksmethreqrcvdrate	<Double>	Read-only	Rate (/s) counter for socksmethreqrcvd

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
socksmethreqsent	<Double>	Read-only	Number of sent SOCKS method request.
socksmethreqsentrate	<Double>	Read-only	Rate (/s) counter for socksmethreqsent
socksmethresprcvd	<Double>	Read-only	Number of received SOCKS method response.
socksmethresprcvdrate	<Double>	Read-only	Rate (/s) counter for socksmethresprcvd
socksmethrespsent	<Double>	Read-only	Number of sent SOCKS method response.
socksmethrespsentrate	<Double>	Read-only	Rate (/s) counter for socksmethrespsent
socksconnreqrcvd	<Double>	Read-only	Number of received SOCKS connect request.
socksconnreqrcvdrate	<Double>	Read-only	Rate (/s) counter for socksconnreqrcvd
socksconnreqsent	<Double>	Read-only	Number of sent SOCKS connect request.
socksconnreqsentrate	<Double>	Read-only	Rate (/s) counter for socksconnreqsent
socksconnresprcvd	<Double>	Read-only	Number of received SOCKS connect response.
socksconnresprcvdrate	<Double>	Read-only	Rate (/s) counter for socksconnresprcvd

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
socksconnrespsent	<Double>	Read-only	Number of sent SOCKS connect response.
socksconnrespsentrate	<Double>	Read-only	Rate (/s) counter for socksconnrespsent
socksservererror	<Double>	Read-only	Number of SOCKS server error.
socksservererrorrate	<Double>	Read-only	Rate (/s) counter for socksservererror
socksclienterror	<Double>	Read-only	Number of SOCKS client error.
socksclienterrorrate	<Double>	Read-only	Rate (/s) counter for socksclienterror
staconnsuccess	<Double>	Read-only	Number of STA connection success.
staconnsuccessrate	<Double>	Read-only	Rate (/s) counter for staconnsuccess
staconnfailure	<Double>	Read-only	Number of STA connection failure.
staconnfailurerate	<Double>	Read-only	Rate (/s) counter for staconnfailure
cpsconnsuccess	<Double>	Read-only	Number of CPS connection success.
cpsconnsuccessrate	<Double>	Read-only	Rate (/s) counter for cpsconnsuccess
cpsconnfailure	<Double>	Read-only	Number of CPS connection failure.
cpsconnfailurerate	<Double>	Read-only	Rate (/s) counter for cpsconnfailure

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
starequestsent	<Double>	Read-only	Number of STA request sent.
starequestsentrate	<Double>	Read-only	Rate (/s) counter for starequestsent
staresponserecvd	<Double>	Read-only	Number of STA response received.
staresponserecvdrate	<Double>	Read-only	Rate (/s) counter for staresponserecvd
icalicensefailure	<Double>	Read-only	Number of ICA license failure.
icalicensefailurerate	<Double>	Read-only	Rate (/s) counter for icalicensefailure
stamonsent	<Double>	Read-only	Number of STA monitor requests sent.
stamonsentrate	<Double>	Read-only	Rate (/s) counter for stamonsent
stamonrcvd	<Double>	Read-only	Number of STA monitor responses recieved.
stamonrcvdrate	<Double>	Read-only	Rate (/s) counter for stamonrcvd
stamonsucc	<Double>	Read-only	Number of STA monitor successful responses.
stamonsuccrate	<Double>	Read-only	Rate (/s) counter for stamonsucc

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
stamonfail	<Double>	Read-only	Number of STA monitor failed responses.
stamonfailrate	<Double>	Read-only	Rate (/s) counter for stamonfail
csgptktvalidatenotstarted	<Double>	Read-only	Total number of STA server lookup failures for auth-id in primary ticket
csgptktvalidatenotstartedrate	<Double>	Read-only	Rate (/s) counter for csgptktvalidatenotstarted
csgrtktvalidatenotstarted	<Double>	Read-only	Total number of STA server lookup failures for auth-id in redundant ticket
csgrtktvalidatenotstartedrate	<Double>	Read-only	Rate (/s) counter for csgrtktvalidatenotstarted
totalsbprequest	<Double>	Read-only	Number of securebrowse requests received
sbprequestrate	<Double>	Read-only	Rate (/s) counter for totalsbprequest
totalsbpsaasrequest	<Double>	Read-only	Number of securebrowse requests received for saas apps
sbpsaasrequestrate	<Double>	Read-only	Rate (/s) counter for totalsbpsaasrequest

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
totalsbpwebrequest	<Double>	Read-only	Number of securebrowse requests received for web apps
sbpwebrequestrate	<Double>	Read-only	Rate (/s) counter for totalsbpwebrequest
totalsbprequestsuccess	<Double>	Read-only	Number of securebrowse requests succeeded
sbprequestsuccessrate	<Double>	Read-only	Rate (/s) counter for totalsbprequestsuccess
totalsbpsaasrequestsuccess	<Double>	Read-only	Number of securebrowse requests succeeded for saas apps
sbpsaasrequestsuccessrate	<Double>	Read-only	Rate (/s) counter for totalsbpsaasrequestsuccess
totalsbpwebrequestsuccess	<Double>	Read-only	Number of securebrowse requests succeeded for web apps
sbpwebrequestsuccessrate	<Double>	Read-only	Rate (/s) counter for totalsbpwebrequestsuccess
totalsbprequestfailure	<Double>	Read-only	Number of securebrowse requests failed
sbprequestfailurerate	<Double>	Read-only	Rate (/s) counter for totalsbprequestfailure

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
totalsbpsaasrequestfailure	<Double>	Read-only	Number of securebrowse requests failed for saas apps
sbpsaasrequestfailurerate	<Double>	Read-only	Rate (/s) counter for totalsbpsaasrequestfailure
totalsbpwebrequestfailure	<Double>	Read-only	Number of securebrowse requests failed for web apps
sbpwebrequestfailurerate	<Double>	Read-only	Rate (/s) counter for totalsbpwebrequestfailure
totalsbpdnsrequestfailure	<Double>	Read-only	Number of DNS failures while using securebrowse protocol
sbpdnsrequestfailurerate	<Double>	Read-only	Rate (/s) counter for totalsbpdnsrequestfailure
totalsbpbackendconnectionfailure	<Double>	Read-only	Number of backend connection failure while using securebrowse requests
sbpbackendconnectionfailurerate	<Double>	Read-only	Rate (/s) counter for totalsbpbackendconnectionfailure
totalsbpconnectorfailure	<Double>	Read-only	Number of times not able to reach connector using

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			securebrowse protocol
sbpconnectorfailurerate	<Double>	Read-only	Rate (/s) counter for totalsbpconnectorfailure
totalcvpnrequest	<Double>	Read-only	Number of cvpn requests received
cvpnrequestrate	<Double>	Read-only	Rate (/s) counter for totalcvpnrequest
totalcvpnsaasrequest	<Double>	Read-only	Number of cvpn requests received for saas apps
cvpnsaasrequestrate	<Double>	Read-only	Rate (/s) counter for totalcvpnsaasrequest
totalcvpnwebrequest	<Double>	Read-only	Number of cvpn requests received for web apps
cvpnwebrequestrate	<Double>	Read-only	Rate (/s) counter for totalcvpnwebrequest
totalcvpnrequestsuccess	<Double>	Read-only	Number of cvpn requests succeeded
cvpnrequestsuccessrate	<Double>	Read-only	Rate (/s) counter for totalcvpnrequestsuccess
totalcvpnsaasrequestsuccess	<Double>	Read-only	Number of cvpn requests succeeded for saas apps
cvpnsaasrequestsuccessrate	<Double>	Read-only	Rate (/s) counter for totalcvpnsaasrequestsuccess

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
totalcvpnwebrequestsuccess	<Double>	Read-only	Number of cvpn requests succeeded for web apps
cvpnwebrequestsuccessrate	<Double>	Read-only	Rate (/s) counter for totalcvpnwebrequestsuccess
totalcvpnrequestfailure	<Double>	Read-only	Number of cvpn requests failed
cvpnrequestfailurerate	<Double>	Read-only	Rate (/s) counter for totalcvpnrequestfailure
totalcvpnsaasrequestfailure	<Double>	Read-only	Number of cvpn requests failed for saas apps
cvpnsaasrequestfailurerate	<Double>	Read-only	Rate (/s) counter for totalcvpnsaasrequestfailure
totalcvpnwebrequestfailure	<Double>	Read-only	Number of cvpn requests failed for web apps
cvpnwebrequestfailurerate	<Double>	Read-only	Rate (/s) counter for totalcvpnwebrequestfailure
totalcvpndnsrequestfailure	<Double>	Read-only	Number of DNS failures while using cvpn
cvpndnsrequestfailurerate	<Double>	Read-only	Rate (/s) counter for totalcvpndnsrequestfailure

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
totalcvpnbackendconnectionfailure	<Double>	Read-only	Number of backend connection failure while using cvpn
cvpnbackendconnectionfailurerate	<Double>	Read-only	Rate (/s) counter for totalcvpnbackendconnectionfailure
totalcvpnconnectorfailure	<Double>	Read-only	Number of times not able to reach connector using cvpn
cvpnconnectorfailurerate	<Double>	Read-only	Rate (/s) counter for totalcvpnconnectorfailure
totaldirectaccessrequest	<Double>	Read-only	Number of directaccess requests received
directaccessrequestrate	<Double>	Read-only	Rate (/s) counter for totaldirectaccessrequest
totaldirectaccessrequestsuccess	<Double>	Read-only	Number of directaccess requests succeeded
directaccessrequestsuccessrate	<Double>	Read-only	Rate (/s) counter for totaldirectaccessrequestsuccess
totaldirectaccessrequestfailure	<Double>	Read-only	Number of directaccess requests failed
directaccessrequestfailurerate	<Double>	Read-only	Rate (/s) counter for totaldirectaccessrequestfailure

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
totaldirectaccessconnectorfailure	<Double>	Read-only	Number of times not able to reach connector using Directaccess
directaccessconnectorfailurerate	<Double>	Read-only	Rate (/s) counter for totaldirectaccessconnectorfailure

Operations

(click to see Properties)

- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/vpn **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/vpn? **args=detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get vpn resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/vpn? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpn": [ {

"cvpnbackendconnectionfailurerate":<Double_value>,

"totalcvpnwebrequest":<Double_value>,

"totalcvpndnsrequestfailure":<Double_value>,

"icalicensefailurerate":<Double_value>,

"stamonrcvdrate":<Double_value>,

"csnonhttpprobehit":<Double_value>,
```

```
"csconnsuccrate":<Double_value>,

"totalcvpnconnectorfailure":<Double_value>,

"iipspillovermipused":<Double_value>,

"totalcvpnwebrequestsuccess":<Double_value>,

"sbpdnsrequestfailurerate":<Double_value>,

"totalcvpnwebrequestfailure":<Double_value>,

"stamonsentrate":<Double_value>,

"socksmethrespsent":<Double_value>,

"totalcvpnrequest":<Double_value>,

"totalcvpnsaasrequestfailure":<Double_value>,

"socksconnresprcvdrate":<Double_value>,

"svpnreqwaftotblock":<Double_value>,

"socksservererrorrate":<Double_value>,

"indexhtmlnoserved":<Double_value>,

"csrequesthit":<Double_value>,

"cshttpprobehitrate":<Double_value>,

"stamonfail":<Double_value>,

"socksservererror":<Double_value>,

"staconnsuccess":<Double_value>,

"dnsreqhitrate":<Double_value>,

"cvpnsaasrequestfailurerate":<Double_value>,

"cfghtmlservedrate":<Double_value>,
```

```
"svpnhttpdcurserverconnectionsopen":<Double_value>,

"dnsreqhit":<Double_value>,

"cpsconnfailure":<Double_value>,

"totalsbprequestfailure":<Double_value>,

"sbpwebrequestsuccessrate":<Double_value>,

"iipdisabledmipusedrate":<Double_value>,

"sbpsaasrequestsuccessrate":<Double_value>,

"vpnlicensefail":<Double_value>,

"totalsbpwebrequestfailure":<Double_value>,

"totalfsrequest":<Double_value>,

"winsrequesthit":<Double_value>,

"indexhtmlhit":<Double_value>,

"iipdisabledmipdisabledrate":<Double_value>,

"sbpsaasrequestfailurerate":<Double_value>,

"stamonfailrate":<Double_value>,

"socksconnrespsent":<Double_value>,

"sbpwebrequestfailurerate":<Double_value>,

"svpnhttpdtotalresponses":<Double_value>,

"csgrtktvalidatenotstarted":<Double_value>,

"cpsconnsuccess":<Double_value>,

"stamonsent":<Double_value>,

"socksmethresprcvdrate":<Double_value>,
```

```
"sbpconnectorfailurerate":<Double_value>,

"totaldirectaccessconnectorfailure":<Double_value>,

"starequestsent":<Double_value>,

"stamonrcvd":<Double_value>,

"iipfailedmipdisabledrate":<Double_value>,

"totalsbpsaasrequestfailure":<Double_value>,

"iipdisabledmipdisabled":<Double_value>,

"staconnfailure":<Double_value>,

"svpnhttpdtotalrequestscachehits":<Double_value>,

"totalcvpnsaasrequest":<Double_value>,

"iipdisabledmipused":<Double_value>,

"cpsconnfailurerate":<Double_value>,

"stamonsuccrate":<Double_value>,

"cvpnrequestsuccessrate":<Double_value>,

"csgtotalconnectedusers":<Double_value>,

"socksconnresprcvd":<Double_value>,

"totalsbpdnsrequestfailure":<Double_value>,

"totalsbpconnectorfailure":<Double_value>,

"directaccessconnectorfailurerate":<Double_value>,

"csrequesthitrate":<Double_value>,

"cvpnwebrequestrate":<Double_value>,

"cshttpprobehit":<Double_value>,
```

```
"directaccessrequestrate":<Double_value>,

"totalsbpwebrequest":<Double_value>,

"staconnsuccessrate":<Double_value>,

"totalsbpsaasrequest":<Double_value>,

"csgptktvalidatenotstartedrate":<Double_value>,

"socksmethreqrcvd":<Double_value>,

"socksmethreqrcvdrate":<Double_value>,

"iipfailedmipused":<Double_value>,

"staresponserecvd":<Double_value>,

"csgptktvalidatenotstarted":<Double_value>,

"icalicensefailure":<Double_value>,

"socksconnreqsentrate":<Double_value>,

"totaldirectaccessrequestfailure":<Double_value>,

"cvpnsaasrequestrate":<Double_value>,

"totalcvpnbackendconnectionfailure":<Double_value>,

"socksconnreqsent":<Double_value>,

"csnonhttpprobehitrate":<Double_value>,

"staresponserecvdrate":<Double_value>,

"iipfailedmipusedrate":<Double_value>,

"sbpsaasrequestrate":<Double_value>,

"cvpndnsrequestfailurerate":<Double_value>,

"socksclienterror":<Double_value>,
```

```
"socksclienterrorrate":<Double_value>,

"cvpnwebrequestsuccessrate":<Double_value>,

"socksmethrespsentrate":<Double_value>,

"fsrequestrate":<Double_value>,

"cvpnrequestrate":<Double_value>,

"totalsbprequestsuccess":<Double_value>,

"sbprequestsuccessrate":<Double_value>,

"starequestsentrate":<Double_value>,

"directaccessrequestsuccessrate":<Double_value>,

"sbprequestfailurerate":<Double_value>,

"sbpwebrequestrate":<Double_value>,

"csgrtktvalidatenotstartedrate":<Double_value>,

"sbpbackendconnectionfailurerate":<Double_value>,

"cfghtmlserved":<Double_value>,

"cvpnrequestfailurerate":<Double_value>,

"staconnfailurerate":<Double_value>,

"socksmethresprcvd":<Double_value>,

"cpsconnsuccessrate":<Double_value>,

"totalcvpnsaasrequestsuccess":<Double_value>,

"socksconnreqrcvdrate":<Double_value>,

"csgconnectedusersrate":<Double_value>,

"totalcsconnsucc":<Double_value>,
```

```
"totalcvpnrequestfailure":<Double_value>,

"socksconnreqrcvd":<Double_value>,

"svpnhttpdtotalrequests":<Double_value>,

"totalsbpsaasrequestsuccess":<Double_value>,

"totalcvpnrequestsuccess":<Double_value>,

"totaldirectaccessrequest":<Double_value>,

"socksmethreqsent":<Double_value>,

"cvpnconnectorfailurerate":<Double_value>,

"sbprequestrate":<Double_value>,

"socksmethreqsentrate":<Double_value>,

"totalsbpwebrequestsuccess":<Double_value>,

"totalsbpbackendconnectionfailure":<Double_value>,

"iipfailedmipdisabled":<Double_value>,

"directaccessrequestfailurerate":<Double_value>,

"totalsbprequest":<Double_value>,

"socksconnrespsentrate":<Double_value>,

"totaldirectaccessrequestsuccess":<Double_value>,

"stamonsucc":<Double_value>,

"winsrequesthitrate":<Double_value>,

"cvpnsaasrequestsuccessrate":<Double_value>,

"iipspillovermipusedrate":<Double_value>,

"cvpnwebrequestfailurerate":<Double_value>
```

```
}]}
```

vpnurlpolicy

Statistics for VPN url policy resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	The name of the vpn urlPolicy for which statistics will be displayed. If not given statistics are shown for all policies. Minimum length = 1
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full
pipolicyhits	<Double>	Read-only	Number of hits on the policy
pipolicyhitsrate	<Double>	Read-only	Rate (/s) counter for pipolicyhits

Operations

(click to see Properties)

- GET (ALL)
- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/vpnurlpolicy **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/vpnurlpolicy? **args=name: <String_value> ,detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get vpnurlpolicy resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/vpnurlpolicy? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnurlpolicy": [ {

"name":<String_value>,

"pipolicyhitsrate":<Double_value>,

"pipolicyhits":<Double_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/stat/vpnurlpolicy/ name_value><String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnurlpolicy": [ {

"name":<String_value>,

"pipolicyhitsrate":<Double_value>,

"pipolicyhits":<Double_value>

}]}
```

vpnvserver

Statistics for VPN virtual server resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name of the virtual server for which to show detailed statistics. Minimum length = 1
clearstats	<String>	Read-write	Clear the statsistics / counters. Possible values = basic, full
primaryipaddress	<String>	Read-only	The IP address on which the service is running.
primaryport	<Integer>	Read-only	The port on which the service is running.
type	<String>	Read-only	Protocol associated with the vserver

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
state	<String>	Read-only	Current state of the server. There are seven possible values: UP(7), DOWN(1), UNKNOWN(2), BUSY(3), OFS(Out of Service)(4), TROFS(Transition Out of Service)(5), TROFS_DOWN(Down When going Out of Service)(8)
totalrequests	<Double>	Read-only	Total number of requests received on this service or virtual server. (This applies to HTTP/SSL services and servers.)
requestsrate	<Double>	Read-only	Rate (/s) counter for totalrequests
totalresponses	<Double>	Read-only	Number of responses received on this service or virtual server. (This applies to HTTP/SSL services and servers.)
responsesrate	<Double>	Read-only	Rate (/s) counter for totalresponses
totalrequestbytes	<Double>	Read-only	Total number of request bytes received on this service or virtual server.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
requestbytesrate	<Double>	Read-only	Rate (/s) counter for totalrequestbytes
totalresponsebytes	<Double>	Read-only	Number of response bytes received by this service or virtual server.
responsebytesrate	<Double>	Read-only	Rate (/s) counter for totalresponsebytes
curtotalvpnusers	<Double>	Read-only	Number of users on this vserver
cursslvpnusers	<Double>	Read-only	Number of aaa sessions on this vserver

Operations

(click to see Properties)

- GET (ALL)
- GET

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.
- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

GET (ALL)

URL: http:// <netscaler-ip-address> /nitro/v1/stat/vpnvserver **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/stat/vpnvserver? **args=name: <String_value> ,detail: <Boolean_value> ,fullvalues: <Boolean_value> ,ntimes: <Integer_value> ,logfile: <String_value> ,clearstats: <String_value>**

Use this query-parameter to get vpnvserver resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/stat/vpnvserver? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnvserver": [ {

"name":<String_value>,

"totalresponsebytes":<Double_value>,

"totalresponses":<Double_value>,

"requestbytesrate":<Double_value>,

"totalrequestbytes":<Double_value>,

"primaryport":<Integer_value>,

"cursslvpnusers":<Double_value>,

"responsesrate":<Double_value>,

"primaryipaddress":<String_value>,

"curtotalvpnusers":<Double_value>,

"responsebytesrate":<Double_value>,

"type":<String_value>,

"state":<String_value>,

"requestsrate":<Double_value>,

"totalrequests":<Double_value>

}]}
```

GET

URL: http:// <netscaler-ip-address> /nitro/v1/stat/vpnvserver/ name_value><String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "vpnvserver": [ {

"name":<String_value>,

"totalresponsebytes":<Double_value>,

"totalresponses":<Double_value>,

"requestbytesrate":<Double_value>,

"totalrequestbytes":<Double_value>,

"primaryport":<Integer_value>,

"cursslvpnusers":<Double_value>,

"responsesrate":<Double_value>,

"primaryipaddress":<String_value>,

"curtotalvpnusers":<Double_value>,

"responsebytesrate":<Double_value>,

"type":<String_value>,

"state":<String_value>,

"requestsrate":<Double_value>,

"totalrequests":<Double_value>
```

```
}]}
```

Citrix ADC Nitro Error Messages

0x300 ERRORS

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_RNAT_INV	769	0x301	Reverse NAT not applicable for default route.
NSERR_INVALID_IF	770	0x302	Invalid interface name/number.
NSERR_MGRLIMIT_REACHED	771	0x303	Maximum manager limit reached.
NSERR_SP_INVALD_TABLE	772	0x304	SP table entries should be in increasing order.
NSERR_RNAT_NATIP_EXISTS	773	0x305	RNAT to the target network with specified NAT IP already exists.
NSERR_RNAT_EXISTS	774	0x306	ACL or NETWORK based RNAT rule already exists.
NSERR_RNAT_NOT_EXISTS	775	0x307	ACL or NETWORK based RNAT rule does not exist.
NSERR_RNAT_NATIP_NOT_EXISTS	776	0x308	RNAT to the target network with specified NAT IP doesn't exist.

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_RNAT_INVALID_NATIP	777	0x309	NAT IP is not valid.
NSERR_RNAT_XACLWITHTTL	778	0x30a	Acl with ttl can not be used in NAT64/ RNAT/RNAT6/ ForwardingSession/ LSN rule.
NSERR_ARP_DISABLED	784	0x310	IP has arp disabled.
NSERR_ARP_SEC_NOT_OWNEDIP	785	0x311	Secondary can not arp for this IP.
NSERR_CPE_RULE_INVAL	786	0x312	Invalid rule.
NSERR_INVAL_FLOWTYPE	787	0x313	Only authorization, audit, VPN session and traffic policies can be bound to aaa user or group.
NSERR_INVAL_POLICY_TYPE	788	0x314	Response rule is invalid in an authorization policy.
NSERR_CPE_RULE_ACTION_INVAL	789	0x315	Request action is valid only for request rule.
NSERR_CPE_DEF_SET_INVAL	790	0x316	Default policy cannot be set.
NSERR_INVAL_FORCECLEANUP	791	0x317	Invalid forcecleanup value.

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_INVAL_AAA_GROUP	792	0x318	Invalid authorizationgroup value.
NSERR_INVAL_PROXY	793	0x319	Invalid allprotocolproxy value.
NSERR_INVAL_HTTPPROXY	800	0x320	Invalid HTTP proxy value.
NSERR_INVAL_FTPPROXY	801	0x321	Invalid FTP proxy value.
NSERR_INVAL_SOCKPROXY	802	0x322	Invalid SOCKS proxy value.
NSERR_INVAL_GOPHERPROXY	803	0x323	Invalid GOPHER proxy value.
NSERR_INVAL_SSLPROXY	804	0x324	Invalid SSL proxy value.
NSERR_INVAL_AAAGRP_MAX	805	0x325	Max 5 groups can be specified in authorizationgroup.
NSERR_INVAL_MAX_PORT_NUM	806	0x326	Maximum 16 ports can be specified in httpport.
NSERR_INVAL_HTTPPORT	807	0x327	Invalid port.
NSERR_INVAL_VPNVSERER_POLTYPE	808	0x328	This type of policy cannot be bound to VPN Vserver.

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_INVAL_VPNGLOBAL_POLTYPE	809	0x329	This type of policy cannot be bound to VPN Global.
NSERR_CPE_REM_INUSE	810	0x32a	Bound policy cannot be removed.
NSERR_PROXY_CONFLICT	811	0x32b	Proxy server for all protocols already configured.
NSERR_PROXY_INVAL	812	0x32c	Domain names allowed only if proxy type is browser
NSERR_PXYEXCPT_INVAL	813	0x32d	Proxy exception allowed only if proxy type is browser
NSERR_CPE_POLTYPE_NO_CSE	814	0x32e	Policy type does not support client security expressions in rule
NSERR_SESSACT_CSE_INCOMPATIBLE	815	0x32f	Session action and rule are incompatible
NSERR_NOMEM_CSE	816	0x330	Not enough memory while adding client security expressions
NSERR_INCOMPAT_FS_RULE	817	0x331	File system expressions supported in authorization policy only
NSERR_INCOMPAT_FS_MIX	818	0x332	Incompatible expressions mixed

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
			with file system expressions in rule
NSERR_DR_ENABLE	819	0x333	Dynamic routing can be enabled on only one IP per subnet
NSERR_MAX_DISTANCE	820	0x334	Only null interface routes can have distance equal to 255
NSERR_NULL_ROUTE_DISTANCE	821	0x335	It is not possible to set the administrative distance/cost metric for a null interface route
NSERR_BAD_ACTION_TCP_PROFILE_TYPE	822	0x336	TCP profile cannot be set to this service type
NSERR_BAD_ACTION_HTTP_PROFILE_TYPE	823	0x337	HTTP profile cannot be set to this service type
NSERR_SP_INVALID_THRESHOLD	824	0x338	Invalid base threshold value
NSERR_VIP_ROUTE_EXISTS	825	0x339	VIP exists for this host route
NSERR_ACTION_BOUND	832	0x340	Action bound to policy can not be deleted.
NSERR_MAX_IPLIMIT	833	0x341	Maximum limit for bound IP to this resource record reached, remaining IP's destined for this

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
			resource record will be discarded.
NSERR_BAD_PREFIX_LEN	826	0x33a	Invalid rnat/lsn network prefix len it must be 0-128
NSERR_INV_NETADDR	827	0x33b	Invalid IPv6 network address
NSERR_MIN_DISTANCE	828	0x33c	Static route cannot have distance less than 1
NSERR_IPSEC_PROFILE_INUSE	829	0x33d	Profile is in use by an ip tunnel.
NSERR_IPSEC_INVALID_PROFILE_NAME	830	0x33e	Invalid profile name.
NSERR_SPOTTED	831	0x33f	Spotted IP cannot be used here
NSERR_IPSEC_PBR_ONLY_IP_SUPPORTED	834	0x342	Only IP range is supported
NSERR_IPSEC_IP_NOT_CONTIGUOUS	835	0x343	Invalid IP range. The IP range does not cover all the IP's for a given subnet mask
NSERR_INVAL_USER_ACCOUNTING	836	0x344	Invalid userAccounting value. userAccounting value must be a radiusPolicy.

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_RDP_PROFILE_INUSE	837	0x345	Profile is in use.
NSERR_RDP_INVALID_PROFILE_NAME	838	0x346	Invalid profile name.
NSERR_RDP_INVALID_RDP_FILE_NAME	839	0x347	RDP file name should have .rdp extension and some special characters for RDP file name are not supported.
NSERR_RDP_INVALID_SERVERPROFILE_NAME	840	0x348	Invalid server profile name.
NSERR_RDP_SERVERPROFILE_ALREADY_IN_USE	841	0x349	Server profile is already in use.
NSERR_AUTO_PROXY_URL_INVALID	842	0x34a	Invalid Autoproxy URL
NSERR_AUTO_PROXY_NO_BROWSER	843	0x34b	Autoproxy URL is allowed only if proxy type is Browser.
NSERR_AUTO_PROXY_CONFLICT	844	0x34c	Both Autoproxy URL and manual proxy parameters (allprotocolproxy, http proxy, ftp proxy, proxy exception list, ...) cannot be configured at same time.

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_RDP_INVALID_HOST_LEN	848	0x350	Invalid Host length. Atleast 3 characters expected
NSERR_RDP_NEED_IP	849	0x351	RDP IP is needed
NSERR_IPSEC_INV_PROF	850	0x352	For IPSEC tunnels, profile name cannot be 'none'
NSERR_RDP_NEED_PSK	854	0x356	PSK is needed
NSERR_IPSEC_ONLY_V1	858	0x35a	Responder Only config is supported with IKEv1
NSERR_RDP_LISTENER_SPECIFY_PORT	859	0x35b	Invalid Listener. Specify Port
NSERR_RDP_INVALID_LISTENER_HOST	860	0x35c	Invalid Listener. Specify valid host, atleast 3 characters expected
NSERR_RDP_LISTENER_INVALID_PORT	861	0x35d	Invalid Listener. Specify valid Port
NSERR_PROXY_NOT_ALLOWED	862	0x35e	Proxy feature not licensed
NSERR_IPSEC_FIPS_UNSUPPORTED_CONFIG	863	0x35f	For IPSEC tunnels in FIPS mode hash algo MD5 or encryption algo 3DES is not supported

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_HOST_RT_GW_NOT_SET	3806	0xede	Host Route Gateway not set

0x850 ERRORS

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_MONITOR_INTERVAL	2128	0x850	Monitor interval must be greater than response timeout
NSERR_MONITOR_DESTIP	2129	0x851	Destination IP must be specified for transparent, tunneled or tos monitors
NSERR_MONITOR_CODES	2130	0x852	Too many response codes, only 16 allowed
NSERR_MONITOR_REF	2131	0x853	Monitor must be unbound before it can be deleted
NSERR_MONITOR_BUILTIN	2132	0x854	Built-in monitors cannot be deleted
NSERR_MONITOR_BOUND	2133	0x855	The monitor is already bound to the service
NSERR_MONITOR_TYPE	2134	0x856	Invalid monitor type
NSERR_MONITOR_LOCAL	2135	0x857	Monitor object cannot be bound to local service

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_TIMEOUT_RANGE	2136	0x858	Timeout value out of range; enter a value between 2 minutes and 1440 minutes
NSERR_INVALIDHASHLEN	2137	0x859	Hashlength should be between 1 and 4096 (inclusive)
NSERR_NOTAUTHORIZED	2138	0x85A	Not authorized to execute this command
NSERR_MONITOR_DEFAULT	2139	0x85B	No operations allowed with the default monitor
NSERR_MONITOR_LDNS_ADD_PERM	2140	0x85C	Cannot add monitor of ldns type
NSERR_MONITOR_LDNS_BIND_PERM	2141	0x85D	Cannot bind ldns monitor
NSERR_BACKUP_LOOP	2144	0x860	The VIP is already a backup in the chain
NSERR_SECURE_UDP	2154	0x86A	Secure mode not supported for this protocol
NSERR_MONITOR_WRONG_TYPE	2155	0x86B	Existing monitor is of different type than given
NSERR_LRTM_PERM	2156	0x86C	Enabling LRTM on this monitor type is not permitted
NSERR_MONITOR_SCRIPTNAME	2157	0x86D	Invalid script name for user monitor

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_MONITOR_DISPATCHERIP	2159	0x86F	Invalid dispatcher IP for user monitor
NSERR_MONITOR_USERPERM	2160	0x870	Operation not permitted for a user monitor
NSERR_MONITOR_NOCODES	2161	0x871	A response code is required for this monitor type
NSERR_INVAL_MON	2162	0x872	Attempt to bind invalid monitor type
NSERR_TYPE_EXISTS	2163	0x873	Only one monitor of this type can be bound to a service
NSERR_MONITOR_UNBIND_DEFAULT	2164	0x874	Default monitor cannot be unbound from a service
NSERR_MONITOR_BIND_DEFAULT	2165	0x875	Default monitor cannot be bound explicitly to a service
NSERR_MONITOR_DISABLE_DEFAULT	2166	0x876	Default monitor cannot be disabled or enabled
NSERR_DRTM_PERM	2167	0x877	Dynamic response timeout is not permitted on this monitor type
NSERR_MON_DTRM_DEVIATION	2168	0x878	Response timeout of the monitor has been changed to interval - 1

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_MONITOR_INVALID_VALUE	2169	0x879	Time parameter must be a multiple of 10
NSERR_MONITOR_NOT_BOUND	2170	0x87A	Monitor not bound to service
NSERR_INVALID_MONITOR	2171	0x87B	Monitor does not exist
NSERR_MONITOR_NO_SUCHIPADDR	2172	0x87C	Some IP addresses were not present
NSERR_MONITOR_SCRIPT_ARG_SIZE	2173	0x87D	Combined argument size too long
NSERR_METRICTABLE_NOENT	2174	0x87E	Metric table does not exist
NSERR_METRICTABLE_EXIST	2175	0x87F	Metric table exists
NSERR_DEL_METRICTABLE_PERMANENT	2176	0x880	Permanent metric table cannot be deleted
NSERR_MAX_METRIC_BINDING	2177	0x881	Maximum of 10 SNMP type metric can be bound to the monitor
NSERR_METRIC_NOENT	2178	0x882	Metric does not exist
NSERR_METRIC_EXISTS	2179	0x883	Metric exists
NSERR_OID_EXIST	2180	0x884	SNMP OID exists
NSERR_SNMP_OID_INVAL	2181	0x885	SNMP OID is invalid

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_METRICTABLE_RDONLY	2182	0x886	No operations allowed on read only metric table
NSERR_THRESHOLD_ZERO	2183	0x887	This metric will not be used for CUSTOM LB as its threshold value is zero
NSERR_LDAP_MONITOR_INCOMPLETE	2184	0x888	bindDN or baseDN must be specified before LDAP monitor can be used
NSERR_MYSQL_MONITOR_INCOMPLETE	2185	0x889	userName or database must be specified before MYSQL monitor can be used
NSERR_POP3_MONITOR_INCOMPLETE	2186	0x88A	userName must be specified before POP3 monitor can be used
NSERR_NNTP_MONITOR_INCOMPLETE	2187	0x88B	group must be specified before NNTP monitor can be used
NSERR_FTPEXTENDED_MONITOR_INCOMPLETE	2188	0x88C	fileName must be specified before FTP-EXTENDED monitor can be used
NSERR_SNMP_MONITOR_INCOMPLETE	2189	0x88D	snmpOID or snmpCommunity must be specified

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
			before SNMP monitor can be used
NSERR_CITRIX_XML_SERVICE	2190	0x88E	application must be specified before CITRIX-XML-SERVICE monitor can be used
NSERR_CITRIX_WEB_INTERFACE	2191	0x88F	sitePath must be specified before CITRIX-WEB-INTERFACE monitor can be used
NSERR_LDNS_MON_CANT_DISABLE	2192	0x890	Atleast one ldns monitor needs to be enabled
NSERR_RES_RETRY_ON_IP_SVR	2193	0x891	Resolve retry can be set only on domain based servers
NSERR_IP_ON_DBS_SVR	2194	0x892	IP Address cannot be set on a domain based server
NSERR_MONITOR_FAILURERETRIES	2196	0x894	Monitor retries must be greater than monitor failureRetries
NSERR_MONITOR_IP	2198	0x896	The server/monitor destination ip address is not appropriate for this monitor
NSERR_MONITOR_SUBNET	2199	0x897	The server/monitor destination ip address should be in

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
			a directly connected subnet for this monitor
NSERR_MONITOR_STATIC	2200	0x898	A static/permanent MAC entry is configured for the server/monitor destination ip address
NSERR_TOSID_NOT_SET	2201	0x899	Tos id must be specified for tos enabled vserver/ monitor
NSERR_FAILURERETRIES_NOT_SUPPORTED	2202	0x89A	The failure retries is not supported for this monitor type. Resetting the value of failure retries to 0(Disabled).
NSERR_SUCCESSRETRIES_NOT_SUPPORTED	2203	0x89B	The success retries is not supported for this monitor type. Resetting the value of success entries to 1(Disabled).
NSERR_SETVS_INVAL_MYSQLPARAMS	2204	0x89C	This parameter is only applicable to a MYSQL vserver.
NSERR_SETVS_INVAL_PROTOCOL_PARAMS	2205	0x89D	The parameters are only applicable to HTTP or SSL vservers.

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_SETVS_INVAL_PROTOCOLS_PARAMS	2206	0x89E	The parameters are only applicable to HTTP, SSL or RTSP vservers.
NSERR_DDC_VALIDATE_CRED_REQUIRED	2207	0x89F	Username, password and ddc domain are required for Xen Desktop monitor\n
NSERR_CITRIX_WI_EXTENDED_MONITOR_INCOMPLETE	2208	0x8A0	userName, password, sitepath and domain must be specified before CITRIX-WI-EXTENDED monitor can be used
NSERR_SETVS_INVAL_MSSQLPARAMS	2209	0x8A1	This parameter is only applicable to a MSSQL vserver.
NSERR_DRTM_MON_BOUNDED_SVC	2210	0x8A2	In a cluster system, deviation can't be set/unset on any already bound monitor.
NSERR_MONITOR_RESP_TO_THRESH	2211	0X8A3	Response timeout threshold is rounded off to nearest multiple of 10 less than the given value
NSERR_PASSIVE_ON_LOAD_ONLY	2212	0x8A4	PASSIVE option can be set only on LOAD monitors.

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_SETVS_INVAL_ORACLEPARAMS	2213	0x8A5	This parameter is only applicable to an ORACLE vserver.
NSERR_RADIUS_ACCOUNTING_MONITOR_INCOMPLETE	2214	0x8A6	Secret key must be specified before RADIUS ACCOUNTING monitor can be used
NSERR_MONITOR_SCRIPT_ARG_CNT	2215	0x8A7	Too many script arguments
NSERR_INVALID_DBSLB_BIND	2216	0x8A8	More than one bind not possible on one service for DBSLB
NSERR_USER_NONETPROF	2217	0x8A9	Netprofile cannot be set on scriptable monitors, so ignoring the configured netprofile for this monitor.
NSERR_MONITOR_NO_SSLPROFILE_BOUND	2218	0x8AA	No SSL profile is attached to monitor. Attach SSL profile first
NSERR_DIAMETER_MONITOR_INCOMPLETE	3550	0xDDE	originHost and originRealm configuration is missing

0x900 ERRORS

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_SVCPORTTYPE	2305	0x901	Service exists with the same port and service type
NSERR_VIP_IN_GROUP	2306	0x902	vserver is bound to a group. Set persistence parameters on group to change them for all vservers in group or unbind vserver from group and set on individual vserver.
NSERR_UNSUPPORTED_BKP	2307	0x903	This backup/primary persistence combination is not supported
NSERR_NONHTTPSSL_VIPINGRP	2308	0x904	Cookie persistence cannot be applied - group has non HTTP/SSL type of vserver
NSERR_NONHTTP_VIPINGRP	2309	0x905	Cookie persistence cannot be applied - group has non-HTTP type of vserver
NSERR_USE_PROPER_RM_CMD	2310	0x906	Use remove IP option instead
NSERR_LBMETHOD_NOT_SUPPORTED	2321	0x911	LB method not supported for LLB/PBR

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_PERSISTENCE_NOT_SUPPORTED	2322	0x912	Persistence not supported for LLB/PBR
NSERR_VSERVER_PARAMETERS	2323	0x913	Vserver arguments not valid for LLB/PBR VIP
NSERR_SERVICE_PARAMETERS	2324	0x914	Service parameters are invalid for LLB/PBR VIP
NSERR_LBVIP_DELETE	2325	0x915	Vserver cannot be removed without removing LB/PBR route
NSERR_CACHEPOLICY_RESPACTION_INVAL	2326	0x916	Integrated caching action cannot be applied on a response
NSERR_CACHELICENSE_FAILED	2327	0x917	The license for Integrated Caching feature was not enabled due to an internal error
NSERR_LBVIP_MULTIROUTES	2328	0x918	VIP can't be associated with multiple LB/PBR routes
NSERR_LBMAC_INVAL	2329	0x919	MAC/IPTUNNEL mode can be set only for a VIP with wildcard IP or with service type ANY or for a sessionless VIP

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_CACHESTATS_OBJ_NOTPRESENT	2336	0x920	No object in cache matching the specified attributes
NSERR_CACHEPOLICY_NOTACTIVE	2337	0x921	Integrated caching policy is not active
NSERR_CACHE_BUILTINS_NOT_SOURCED	2338	0x922	Failed sourcing cache builtins, Disabling IC
NSERR_CACHEPOLICY_PRIORITY_INVAL	2339	0x923	Invalid priority
NSERR_ROUTE6_DEFAULT_ONLY	2340	0x924	Only default route configuration supported
NSERR_ROUTE6_DEFAULT_EXISTS	2341	0x925	Configured route already exists
NSERR_ROUTE6_INVALID_GATEWAY	2342	0x926	Invalid gateway
NSERR_ROUTE6_MAX	2343	0x927	Already maximum number of routes configured
NSERR_ROUTE6_NOT_EXIST	2344	0x928	Route does not exist
NSERR_IPV6_INVALID_ADDR	2345	0x929	Incorrect IPv6 address type
NSERR_LBVIP_IPV6TOV4	2352	0x930	Changing IP from IPv6 to IPv4 not permitted

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_IPV6_NSIPTOVIP	2353	0x931	Configuring NSIP as VIP not permitted
NSERR_IPV6_VIPTONSIP	2354	0x932	Configuring VIP as NSIP not permitted
NSERR_IPV6_SCOPE	2355	0x933	Incorrect IPv6 address scope. (Default: global)
NSERR_LBVIP_IPV4TOV6	2356	0x934	Changing IP from IPv4 to IPv6 not permitted
NSERR_IPV6_LINKLOCALTOVIP	2357	0x935	Configuring Link-Local address as VIP not permitted
NSERR_IPV6_MAPIPONNSIP	2358	0x936	Mapped IP should not be configured for NSIP (Ignoring mapped ip)
NSERR_SECUREIPPORTADDRINUSE	2359	0x937	Internal secure service exists with the same port and service type. Please use this for secure access
NSERR_IPV6_INVALID_PREFIX	2360	0x938	Link-local prefix length is not equal to 64
NSERR_ND6_LINKLOCAL_VLAN	2361	0x939	Vlan is necessary with IPv6 Link-local address
NSERR_INVALID_IPV6_PREFIXLFT	2362	0x93A	Invalid IPv6 prefix life time. prefix valid life time must be greater

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
			than or equal to preferred life time
NSERR_IPV6_ND_TIMEOUT	2363	0x93B	Can not SET/UNSET ndtimeouts, when ra_learning is enabled.
NSERR_ND6_VLAN_INTF	2368	0x940	Interface/channel not a member of given vlan
NSERR_PERSIST_TIMEOUT_TO_DEFAULT	2369	0x941	Unsetting Persistency, changing timeout to default
NSERR_LB_GROUP_NOT_EXIST	2370	0x942	LB group does not exist
NSERR_LB_VSERVER_ALREADY_BOUND	2371	0x943	Vserver is already bound to an LB group
NSERR_ROUTE6_INVALID_LINKLOCAL_GATEWAY_VLAN	2372	0x944	Vlan ID must be specified for linklocal gateway
NSERR_ROUTE6_NO_GWORIF	2373	0x945	Either Gateway or Interface (vlan) should be specified for route
NSERR_ROUTE6_VLAN_MONITOR	2374	0x946	Monitor should not be given for vlan route
NSERR_LBMETHOD_LEASTREQ_NOT_SUPPORTED	2375	0x947	LeastRequest LB method not supported for this service type

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_IPV6_MULTIPLE_LLIP	2376	0x948	Multiple link-local IPs to a Vlan is not allowed
NSERR_IPV6_TOOMANY_PREFIXES	2377	0x949	Too many prefixes to a Vlan, maximum 5 prefixes are allowed
NSERR_RAPREFIX_BOUNDTOVLAN	2378	0x94A	Router Advertisement prefix is bound to vlan
NSERR_LB_VSERVER_NOT_BOUND	2379	0x94B	Given vserver is not bound to this LB group
NSERR_VSERVER_BOUND_TO_NG	2380	0x94C	Cannot delete vserver that is bound to a nodegroup
NSERR_LRMINTHROUGHPUT_ONLACPONLY	2382	0x94E	Link Redundancy minimum throughput can be set only on LACP Channels
NSERR_CACHE_POLICY_CONTENTGRPMISMATCH	2383	0x94F	Type of Content Group and Policy does not Match.
NSERR_NONHTTPNOSQL_VS	2384	0x950	Specified policy can be bound only to HTTP/SSL/ HTTP_QUIC// MYSQL/MSSQL/ PROXY vserver.
NSERR_SMPP_CUSTOM_SVRID_LEN_NOT_SUPPORTED	2385	0x951	CustomServerID length for SMPP protocol must be 2

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_SMPP_CUSTOM_SVRID_NOT_EXIST	2386	0x952	CustomServerID is mandatory for SMPP protocol
NSERR_SMPP_CUSTOM_SVRID_EXIST	2387	0x953	CustomServerID already exists, it should be unique for SMPP protocol
NSERR_SIP_DUPLICATE_SRC_PORT	2388	0x954	RNAT source port and RNAT secure source port must be different
NSERR_SIP_DUPLICATE_DST_PORT	2389	0x955	RNAT destination port and RNAT secure destination port must be different
NSERR_IP_ADDR_ICMP_DIS_NOT_ALLOWED	2390	0x956	Disabling ICMP for an IP(v6) address is not allowed
NSERR_IP_ADDR_ND6_DIS_NOT_ALLOWED	2391	0x957	disabling neighbor discovery for an ipv6 address is not allowed
NSERR_IP_ADDR_STATE_DIS_NOT_ALLOWED	2392	0x958	state disable is not allowed for an IP(v6) address
NSERR_ND6_LOOP_LL_NOT_ALLOW	2393	0x959	Loopback/self or link-local IP addresses not allowed
NSERR_PERSISTENCE_NOT_SUPPORTED_ON_GROUP	2417	0x971	Vserver level persistency is enabled on the group. Set Persistence

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
			parameters on bound vservers.
NSERR_ARGS_AAA_OTP	2420	0x974	authentication can not be ENABLED when otpsecret is specified
NSERR_ARGS_AAA_SSHPUBKEY	2421	0x975	authentication can not be ENABLED when sshPubKey is specified
NSERR_CLOUD_CRED	2422	0x976	Unable to connect to the cloud. Check credentials.
NSERR_CLOUD_NSCRED	2423	0x977	Unable to issue NITRO API calls.
NSERR_SECTYPE_PLAINTEXT	2424	0x978	validateServerCert configuration not allowed when secType is PLAINTEXT.
NSERR_ARGS_AAA_HASH_ATTRIB	2425	0x979	Value to is Invalid. Either an attribute has more than 127 bytes or total string exceeds 2047 bytes
NSERR_CLOUD_DNS	2432	0x980	Unable to connect to the cloud. DNS resolution failed.
NSERR_CLOUD_FSERR	2433	0x981	Unable to validate cloud credentials. Access error.

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_REDIRECTION_INVALID	2434	0x982	Mac mode redirection setting on Vserver should not be enabled for LLB config.

ACL ERRORS

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_ACL_NOT_EXISTS	864	0x360	ACL rule does not exist
NSERR_ACL_EXISTS	865	0x361	IP address has existing ACL rule
NSERR_ACLPIP_WOSRCDST	866	0x362	Peer IP can't be given without src/dst flag
NSERR_ACL_SAMEIP_PIP	867	0x363	IP address and peer IP can't be same
NSERR_ACL_INVAL_PEERIP	868	0x364	Invalid peer IP
NSERR_ACL_IPPIP_EXISTS	869	0x365	ACL with identical parameter specification already exists
NSERR_XACLDELERROR	870	0x366	ACL has already been removed
NSERR_XACLADDERROR	871	0x367	Src/DstPort or RedirectPort can be specified only if protocol is TCP (6) or UDP (17)

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_XACL_PRIORITY_EXISTS	872	0x368	ACL with this priority already exists
NSERR_XACL_ICMP_REQD	873	0x369	ICMP type / code can be specified only if protocol is ICMP(1)
NSERR_NOLOOPBACK	874	0x36a	ACL cannot be configured on the loopback interface
NSERR_INVICMPTYPE	875	0x36b	Invalid ICMP type
NSERR_INVICMPCODE	876	0x36c	Invalid ICMP code
NSERR_XACLRNATDEL	877	0x36d	ACL is bounded to RNAT/LSN, cannot be removed
NSERR_XACLMODCFGINFO	878	0x36e	ACL modified, apply ACLs to activate change
NSERR_XACLFWDSESSIONDEL	879	0x36f	ACL is bounded to FORWARDSESSION, cannot be removed

ACL6 ERRORS

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_ACL6_IPPIP_EXISTS	896	0x380	ACL6 with identical parameter specification already exists

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_ACL6_DELERROR	897	0x381	ACL6 has already been removed
NSERR_ACL6_ADDERROR	898	0x382	Port can be specified only if protocol is TCP (6) or UDP (17)
NSERR_ACL6_PRIORITY_EXISTS	899	0x383	ACL6 with this priority already exists
NSERR_ACL6_ICMP_REQD	900	0x384	ICMPv6 type/code can be specified only if protocol is ICMPv6 (58)
NSERR_ACL6_UNSPECADDR	901	0x385	unspecified address (::) can not be configured in ACL6
NSERR_ACL6_MODCFGINFO	902	0x386	ACL6 modified, apply ACLs6 to activate change
NSERR_ACL6_PREFIXLEN	903	0x387	Prefix length should not be configured in ACL6. (Use range instead)
NSERR_ACL6_RNAT_NOT_ALLOWED	904	0x388	Action must be ALLOW to bind ACL6 to RNAT
NSERR_ACL6RNAT_DELERROR	905	0x389	This ACL6 is associated with rnat6/nat64/forwardingsession/lsn config, Remove rnat6/nat64/forwardingsession/lsn first

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_RNAT6_INVALID_REDPORT	906	0x38a	Invalid option for SET/UNSET, redirect port can be specified only for acl6 based RNAT
NSERR_ACL6_RNAT_EXISTS	907	0x38b	ACL6 based rnat is already exist for this acl6(Duplicate config)
NSERR_NET_RNAT6_EXISTS	908	0x38c	Network based rnat/lsn already exists for this network address(Duplicate config)
NSERR_RNAT_VIP_PORT_ALLOC_FAIL	909	0x38d	ERROR : Port allocation for VIP v6 address Failed
NSERR_ACL6_RNAT_NAT64_NOT_ALLOWED	910	0x38e	ERROR : Acl6 already bound to nat64 config
NSERR_ACL_SRCMAC_MASK_LENGTH	911	0x38f	SrcMacMask length should be 12
NSERR_ACL_INVALID_NAME	1444	0x5a4	ERROR : ACL name length should be >=1 and <=128
NSERR_ACL_SRCMAC_MASK_PAIR	1455	0x5af	SrcMacMask should Contain consecutive 1s or 0s per octet and pair of 0s should not be present after pair of 1s

ADTCP ERRORS

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_ADTCP_PROFILE_NOT_FOUND	3781	0xec5	AdaptiveTCP profile not found
NSERR_ADTCP_PROFILE_INVALID	3792	0xed0	Invalid AdaptiveTCP profile
NSERR_ADTCP_CQARULE_NAME_INUSE	3793	0xed1	Rule name already in use

APPFLOW ERRORS

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_APPFLOW_INVALIDPORT	3936	0xf60	Invalid collector port
NSERR_NO_SUCH_COLLECTOR	3938	0xf62	No matching collector
NSERR_APPFLOW_METRICS_ACTION	3939	0xf63	Set operation is not allowed on Appflow action with metricsLog option enabled.
NSERR_APPFLOW_NONZERO_REFCOUNT	3940	0xf64	The AppFlow entity is in use.
NSERR_APPFLOW_COLLECTOR_NAME_INUSE	3941	0xf65	AppFlow collector name already in use.
NSERR_APPFLOW_ACT_INVAL	3942	0xf66	No such AppFlow action exists.

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_APPFLOW_NETPROF_REQD	3472	0xd90	NetProfile required for AppFlow collector within partition.
NSERR_COLLECTOR_TRANSPORT_MISMATCH	1220	0x4c4	All collectors attached to an action should have the same transport type.
NSERR_SAME_TYPE_PROFILE_BOUND	1221	0x4c5	Two profiles of same type cannot be bound.
NSERR_COLLECTOR_LOGSTREAM	1222	0x4c6	ANOMALOUS transaction option is valid only with Logstream collector.
NSERR_HTTP_STREAM	1225	0x4c9	Only REST type collectors are allowed with this profile.
NSERR_PROFILE_TYPE_MISMATCH	1226	0x4ca	Invalid profile type.
NSERR_ENABLE_IPFIX_LOGGING	1227	0x4cb	IPFIX logging not enabled.
NSERR_BOUNDTO_ANALYTICS	1228	0x4cc	Bound to analytics entity.
NSERR_HTTP_SVC_ONLY	1229	0x4cd	Only HTTP service is allowed with this profile.
NSERR_REST_COL_PROFILE	1230	0x4ce	Either one of REST collector or HTTP-Stream profile can be active at a time.

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_PROFILE_TYPE_EXISTS	1231	0x4cf	Only one profile of this type can exist.
NSERR_INVALID_APPFLOW_TRANSPORT	1245	0x4dd	Invalid service-type. Only Logstream and IPFIX are allowed.
NSERR_COLLECTOR_DUPLICATES	1267	0x4f3	Duplicate collectors not allowed.
NSERR_MULTIPLE_EVENTS_AUDITS_CONFIG	1268	0x4f4	Events and Auditlogs can be enabled on only one time series profile
NSERR_NO_CONTENT_TYPE	1269	0x4f5	Content Type has to be specified for a collector at least once
NSERR_NO_ENDPOINT_URL	1270	0x4f6	Endpoint URL has to be specified for a collector at least once
NSERR_REF_NO_MOD	1271	0x4f7	The collector is already referenced somewhere else and thus the collector properties cannot be modified.
NSERR_INVALID_DATA_FILE	1272	0x4f8	Invalid Data Format File.
NSERR_HDR_REPEATED	1274	0x4fa	Custom header name repeated.
NSERR_RM_CSPS_KEK_CONFIRM	1275	0x4fb	Encrypted configuration cannot be recovered if Key

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
			Encryption Key is removed. Do you want to proceed? (Y/N) [N]:
NSERR_RM_CSPS_SSH_CONFIRM	1276	0x4fc	SSH connections to the ADC will be affected. System needs to be rebooted to create new SSH host keys. Do you want to proceed? (Y/N) [N]:
NSERR_INVALID_JSON_INPUT	1277	0x4fd	Invalid JSON Schema file

AS ERRORS

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_AS_NOSTARTURL	3120	0xc30	No such StartURL check
NSERR_AS_EXIST_STARTURL	3121	0xc31	The StartURL check is already in use
NSERR_AS_NODENYURL	3122	0xc32	No such DenyURL check
NSERR_AS_EXIST_DENYURL	3123	0xc33	The DenyURL check is already in use
NSERR_AS_NOCOOKIECONSISTENCY	3124	0xc34	No such CookieConsistency check

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_AS_EXIST_COOKIECONSISTENCY	3125	0xc35	The CookieConsistency check is already in use
NSERR_AS_NOFIELDCONSISTENCY	3126	0xc36	No such FieldConsistency check
NSERR_AS_EXIST_FIELDCONSISTENCY	3127	0xc37	The FieldConsistency check is already in use
NSERR_AS_NOXSS	3128	0xc38	No such CrossSiteScripting check
NSERR_AS_EXIST_XSS	3129	0xc39	The CrossSiteScripting check is already in use
NSERR_AS_NOSQL	3130	0xc3a	No such SQLInjection check
NSERR_AS_EXIST_SQL	3131	0xc3b	The SQLInjection check is already in use
NSERR_AS_NOFIELDFORMAT	3132	0xc3c	No such FieldFormat check
NSERR_AS_EXIST_FIELDFORMAT	3133	0xc3d	The FieldFormat check is already in use
NSERR_AS_NOOBJECTEXPRESSION	3134	0xc3e	No such SafeObject check

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_AS_EXIST_OBJECTEXPRESSION	3135	0xc3f	The SafeObject check is already in use
NSERR_AS_NOFIELDTYPE	3136	0xc40	No such FieldType. See /var/log/ns.log for more details.
NSERR_AS_NOT_SUPPORTED_VS	3137	0xc41	Specified policy can be bound only to HTTP/SSL/HTTP_QUIC/PROXY vserver
NSERR_AS_BAD_ACTION_STARTURL	3138	0xc42	Invalid StartURL Action
NSERR_AS_BAD_ACTION_DENYURL	3139	0xc43	Invalid DenyURL Action
NSERR_AS_BAD_ACTION_COOKIECONSISTENCY	3140	0xc44	Invalid CookieConsistency Action
NSERR_AS_BAD_ACTION_FIELDCONSISTENCY	3141	0xc45	Invalid FieldConsistency Action
NSERR_AS_BAD_ACTION_XSS	3142	0xc46	Invalid CrossSiteScripting Action
NSERR_AS_BAD_ACTION_SQL	3143	0xc47	Invalid SQLInjection Action
NSERR_AS_BAD_ACTION_FIELDFORMAT	3144	0xc48	Invalid FieldFormat Action

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_AS_BAD_ACTION_OBJECTEXPRESSION	3145	0xc49	Invalid SafeObject Action
NSERR_AS_BAD_ACTION_BUFFEROVERFLOW	3146	0xc4a	Invalid BufferOverflow Action
NSERR_AS_BAD_ACTION_CCARD	3147	0xc4b	Invalid CreditCard Action
NSERR_AS_FIELDFORMAT_MIN_GT_MAX	3148	0xc4c	Minimum FieldFormat length cannot exceed maximum FieldFormat length
NSERR_AS_FIELDTYPE_BAD_NAME_LEN	3149	0xc4d	Invalid FieldType name length
NSERR_AS_BAD_COMMENT_LEN	3150	0xc4e	Invalid comment length
NSERR_AS_FIELDTYPE_BAD_REGEX_LEN	3151	0xc4f	Invalid regex length
NSERR_AS_SECURITY_CHECK_REQUIRED	3152	0xc50	Security check required
NSERR_AS_FIELDTYPE_BUILTIN	3153	0xc51	Built-in FieldTypes cannot be modified or deleted
NSERR_AS_BAD_ACTION_CONTENT_TYPE	3154	0xc52	Invalid ContentType Action

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_AS_BAD_DEFAULT_CHARSET	3155	0xc53	Invalid default character set
NSERR_AS_BAD_COOKIECONSISTENCY_NAME	3156	0xc54	Invalid Cookie name
NSERR_AS_BAD_ERRORURL	3157	0xc55	Invalid ErrorURL
NSERR_AS_BAD_ENCODING_URL	3158	0xc56	Invalid encoding for URL
NSERR_AS_BAD_ENCODING_FIELDNAME	3159	0xc57	Invalid encoding for field name
NSERR_AS_BAD_ENCODING_COOKIENAME	3160	0xc58	Invalid encoding for cookie name
NSERR_AS_BAD_ENCODING_OBJECTEXPRESSION_NAME	3161	0xc59	Invalid encoding for SafeObject name
NSERR_AS_BAD_ENCODING_EXPRESSION	3162	0xc5a	Invalid encoding for expression
NSERR_AS_BAD_ENCODING_REGEX	3163	0xc5b	Invalid encoding for regex
NSERR_AS_MODIFIED_URL	3164	0xc5c	Replaced character that is not printable ASCII with escaped equivalent in URL

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_AS_MODIFIED_OBJECTEXPRESSION	3165	0xc5d	Replaced character that is not printable ASCII with escaped equivalent in expression
NSERR_AS_CFFIELD_BAD_FIELDNAME_LEN	3166	0xc5e	Invalid confidential form field name length
NSERR_AS_CFFIELD_BAD_URL_LEN	3167	0xc5f	Invalid confidential form field URL length
NSERR_AS_NOCFFIELD	3168	0xc60	No such confidential form field
NSERR_AS_BAD_CFF_NAME	3169	0xc61	Name may not contain leading/ trailing spaces.
NSERR_AS_BAD_CFF_URL	3170	0xc62	URL may not contain leading/trailing spaces.
NSERR_AS_CFF_DUP	3171	0xc63	The confidential field is already in use.
NSERR_AS_BAD_ACTION_XDOS	3172	0xc64	Invalid XML Dos Action
NSERR_AS_EXIST_XML_DOS_URL	3173	0xc65	The XML DoS URL check is already in use.
NSERR_XML_URL_NOT_SUPPORTED	3174	0xc66	Only .* is supported for XML checks.
NSERR_AS_NO_XDOS_URL	3175	0xc67	No such URL exist for XDOS check.

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_AS_INVALID_XML_DOS_CONF	3176	0xc68	Invalid configuration: xmlMaxFileSize can not be less than xmlMinFileSize when both checks are enabled.
NSERR_AS_BAD_ACTION_XML_SQLINJECTION	3177	0xc69	Invalid XML - SQLInjection Action.
NSERR_AS_BAD_ACTION_XML_XSS	3178	0xc6a	Invalid XML - CrossSiteScripting Action.
NSERR_AS_BAD_ACTION_XML_WELLFORMEDNESS	3179	0xc6b	Invalid XML - Format Action.
NSERR_AS_BAD_ACTION_PROFILE_TYPE	3180	0xc6c	Invalid Appsecure Profile Type.
NSERR_AS_MODIFIED_FIELDNAME	3181	0xc6d	Replaced character that is not printable ASCII with escaped equivalent in form field name
NSERR_AS_BAD_ACTION_WSI	3182	0xc6e	Invalid XML WS-I Action.
NSERR_AS_EXIST_XML_WSI_URL	3183	0xc6f	The XML WS-I URL check is already in use.
NSERR_AS_NO_WSI_URL	3184	0xc70	No such URL exist for WS-I check.

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_AS_INVALID_XML_WSI_CONF	3185	0xc71	Invalid WS-I rule id in the list.
NSERR_AS_OBJECTNAME_TOO_BIG	3186	0xc72	Object too big.
NSERR_AS_OBJECT_NO_EXIST	3187	0xc73	Imported file does not exist [Please import the file before use]. See /var/log/ns.log for more details.
NSERR_AS_SERVER_NAME_TOO_BIG	3188	0xc74	Server name too big.
NSERR_AS_OBJECT_NOT_READABLE	3189	0xc75	Object not readable [Please make sure it exists].
NSERR_AS_NOPROFILE	3190	0xc76	No such profile.
NSERR_AS_BAD_ACTION_XML_ATTACHMENT	3191	0xc77	Invalid XML - Attachment Action
NSERR_AS_BAD_ACTION_MSGVAL	3192	0xc78	Invalid XML Message Validation Action.
NSERR_AS_EXIST_XML_MSGVAL_URL	3193	0xc79	The XML MSGVAL URL check is already in use.
NSERR_AS_NO_MSGVAL_URL	3194	0xc7a	No such URL exist for MSGVAL check.

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_AS_INVALID_XML_MSGVAL_CONF	3195	0xc7b	Invalid MsgVal configuration.
NSERR_AS_BIND_XML_MSGVAL_CONF	3196	0xc7c	Error in message validation binding. For More details see log messages.
NSERR_AS_IMPORT_FAILED	3197	0xc7d	Importing the resource failed
NSERR_AS_OBJECT_EXIST	3198	0xc7e	Object already exists
NSERR_AS_INVALID_OPTION	3199	0xc7f	Invalid option
NSERR_AS_REMOVE_FAILED	3200	0xc80	Problem in removing resource
NSERR_AS_NO_RESOURCE	3201	0xc81	No such resource. Object you are trying to update or remove does not exist.
NSERR_AS_SHOW_FAILED	3202	0xc82	Problem in showing object
NSERR_AS_DEPENDENCY_FAILED	3203	0xc83	Problem in downloading dependencies
NSERR_AS_COMPILATION_FAILED	3204	0xc84	Problem compiling object. For more details see /var/log/ns.log file
NSERR_INVALID_OBJECT_NAME	3205	0xc85	Invalid name; names must begin with an alphanumeric

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
			character or underscore and must contain only alphanumerics, '_', '#', '.', ':', '@', '=' or '-'
NSERR_AS_IMPORT_DOWNLOAD_FAILED	3206	0xc86	Problem in importing the object. Please check the DNS NameServer/Route settings and try again. For more details see /var/log/ns.log file
NSERR_AS_RESOURCE_INUSE	3207	0xc87	Can not remove resource. Resource is in use
NSERR_AS_BAD_MAPPING_DATA	3208	0xc88	Mapping Data Corrupted
NSERR_AS_PROFILE_CHANGE_HTML	3209	0xc89	HTML checks will not be applicable when profile type is not HTML
NSERR_AS_PROFILE_CHANGE_XML	3210	0xc8a	XML checks will not be applicable when profile type is not XML
NSERR_AS_IMPORT_ALREADY_INPROCESS	3211	0xc8b	Import failed. Another resource with the same name being processed
NSERR_AS_INVALID_XML_ERROR_OBJECT	3212	0xc8c	Invalid XML error object

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_AS_XML_WELLFORMEDNESS_DISABLED	3213	0xc8d	XML Security checks can not be performed, once an XML message is found not wellformed.
NSERR_AS_INDIVIDUAL_IMPORT_LIMIT_EXCEEDED	3214	0xc8e	Import failed - importing file size greater than configured size limit
NSERR_AS_TOTAL_IMPORT_LIMIT_EXCEEDED	3215	0xc8f	Import failed - exceeding the configured total size limit on the imported objects
NSERR_AS_LEARNING_BUSY	3216	0xc90	Please wait for the learning database to finish updating
NSERR_AS_DEPRECATED_XML_WSI_RULE_R4003	3217	0xc91	WS-I Rule R4003 has been deprecated, it will be removed from the WS-I binding list.
NSERR_AS_EXIST_XML_ATTACHMENT_URL	3218	0xc92	The XML Attachment URL check is already in use.
NSERR_AS_NO_XML_ATTACHMENT_URL	3219	0xc93	No such URL exist for XML Attachment check.
NSERR_AS_BAD_ACTION_SOAP_FAULT	3220	0xc94	Invalid SOAP Fault Filtering Action.

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_AS_XML_DOS_VALUE_OUT_OF_RANGE	3221	0xc95	XML DoS check value is not within the allowed range.
NSERR_AS_XML_MSGVAL_CLI_ERROR	3222	0xc96	-XMLValidateResponse requires one of [-XMLValidateSOAPEnvelope, -XMLWSDL, -XMLRequestSchema, -XMLResponseSchema]
NSERR_AS_INVALID_CUSTOM_SETTINGS_OBJECT	3223	0xc97	Import failed. Please check syntax of signature object
NSERR_AS_SESSION_TIMEOUT_LIFETIME_CONFLICT	3224	0xc98	The session lifetime cannot be less than the session timeout
NSERR_AS_CLASSIC_POLICY_ALREADY_BOUND	3225	0xc99	Failed to bind advanced policy because a classic one is already bound globally or to a vserver. Binding classic and advanced policies at the same time is not allowed
NSERR_AS_ADVANCED_POLICY_ALREADY_BOUND	3226	0xc9a	Failed to bind classic policy because an advanced one is already bound globally or to a vserver or to a user defined policylabel.

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
			Binding classic and advanced policies at the same time is not allowed
NSERR_AS_CUSTOM_SETTINGS_NO_INJECTION_TYPE	3227	0xc9b	Failed to set signature object. One of the tags do not have 'type' attribute
NSERR_AS_NOCSRF_TAG	3228	0xc9c	No such CrossSiteRequestForgery check
NSERR_AS_EXIST_CSRF_TAG	3229	0xc9d	The CrossSiteRequestForgery check is already in use
NSERR_AS_BAD_ACTION_CSRF_TAG	3230	0xc9e	Invalid CSRF Tag Action
NSERR_AS_TURNING_TAGGING_OFF_CSRF_TAG_ON	3231	0xc9f	Must set CSRF tagging check to 'none' before disabling form tagging.
NSERR_AS_TURNING_CSRF_TAG_ON_TAGGING_OFF	3232	0xca0	Form tagging must be enabled before turning on CSRF tag checks.
NSERR_AS_IMPORT_LIMIT_LESS_THAN_IMPORT_DIR_SIZE	3233	0xca1	Import limit should be greater than the current total imported objects size.

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_AS_UNSUPPORTED_IMPORT_PROTOCOL	3234	0xca2	Unsupported import source protocol. Supported protocols are http, https and ftp
NSERR_AS_UNSUPPORTED_EXPORT_PROTOCOL	3235	0xca3	Unsupported export target protocol. Supported protocols are http and https
NSERR_AS_EXPORT_FAILED	3236	0xca4	Export failed. Check /var/log/ns.log for details.
NSERR_AS_BAD_LOCAL_FILE	3237	0xca5	Local URI cannot be empty and should not contain ../ or ? or #
NSERR_AS_INVALID_REGEX_CUSTOM_OBJECT	3238	0xca6	Invalid regular expression in custom object. Reverting to default settings.
NSERR_AS_BUILTIN_INVALID_OP	3239	0xca7	Invalid operation for built-in profile
NSERR_AS_INVALID_ADV_POLICY_STATE	3240	0xca8	Cannot bind advanced policy with state set to DISABLED
NSERR_AS_BUILTIN_NAMES_IN_CONF	3241	0xca9	Entities with names reserved for built-in profiles have been discarded
NSERR_AS_NO_LEARN_DENYURL	3243	0xcab	Learn is not supported as a denyURLAction.

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_AS_INVALID_XML_FILE_SIZE	3244	0xcac	Invalid configuration: xmlMinFileSize / xmlMaxFileSize can not be less than 4 or greater than 1000000000.
NSERR_AS_NO_LEARN_BUFFEROVERFLOW	3246	0xcae	Learn is not supported as a bufferOvewflowAction.
NSERR_AS_NO_LEARN_XML_FORMAT	3247	0xcaf	Learn is not supported as an XMLFormatAction.
NSERR_AS_NO_LEARN_XML_SQLINJECTION	3251	0xcb3	Learn is not supported as an XMLSQLInjectionAction.
NSERR_AS_BAD_ACTION_MULTIPLE_HEADER	3252	0xcb4	Invalid Multiple Header Action. Only one of Block and KeepLast is allowed / None cannot be used with another Multiple Header Action.
NSERR_AS_NO_LEARN_XML_MSGVAL	3253	0xcb5	Learn is not supported as an XMLValidationAction.
NSERR_AS_NO_LEARN_XML_SOAP_FAULT	3254	0xcb6	Learn is not supported as an XMLSOAPFaultAction.

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_AS_IMPORT_INTERNAL_ERROR	3255	0xcb7	Internal error while importing resource.
NSERR_AS_NETSVC_CONN_FAILED	3256	0xcb8	Critical internal error. please retry after some time.
NSERR_AS_VALIDATION_FAILED	3257	0xcb9	Problem validating Imported object against specification. For more details see /var/log/ns.log file.
NSERR_AS_CKI_TRANSFORM_DISABLED	3258	0xcba	This setting will not take effect until cookieTransforms is turned ON.
NSERR_AS_NOXMLXSS	3259	0xcbb	No such XMLXSS check
NSERR_AS_EXIST_XMLXSS	3260	0xcbc	The XMLXSS check is already in use
NSERR_AS_NOXMLSQL	3261	0xcbd	No such XMLSQLInjection check
NSERR_AS_EXIST_XMLSQL	3262	0xcbe	The XMLSQLInjection check is already in use
NSERR_AS_NO_ENDTAG	3263	0xcbf	Missing end tag in the imported signature file.

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_AS_SIG_INVALID_RULEID	3264	0xcc0	Invalid rule id in imported signature. Rule id must be between 1 and 2, 147, 483, 647.
NSERR_AS_SIG_INVALID_RULE_VERSION	3265	0xcc1	Invalid version in imported signature.
NSERR_AS_SIG_PARSE_ERROR	3266	0xcc2	Error parsing imported signatures.
NSERR_AS_SIG_INVALID_ATTRIBUTE	3267	0xcc3	Imported signatures have invalid attributes
NSERR_AS_SIG_MULTIPLE_LOCATIONS	3268	0xcc4	Imported signature patterns has multiple locations
NSERR_AS_SIG_INVALID_STATE	3269	0xcc5	Error parsing imported signatures. Invalid parse state.
NSERR_AS_CKI_ENCRYPT_METHOD_IS_NONE	3270	0xcc6	For security purposes, please set the NS encryptions parameter using the \"set ns encryptionParams\" command.
NSERR_AS_UPDATE_FAILED	3271	0xcc7	Updating the resource failed
NSERR_AS_OBJECT_NOT_USED	3272	0xcc8	The specified object is not used

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_AS_SIG_MULTIPLE_URLS	3273	0xcc9	Imported signature pattern location has multiple URLs
NSERR_AS_SIG_MULTIPLE_FIELD_NAMES	3274	0xcca	Imported signature pattern location has multiple field names
NSERR_AS_SIG_NO_FASTMATCH	3275	0xccb	A signature rule has no fastmatch pattern. See log for details.
NSERR_AS_PE_POLICY_NOTSUPPORTED	3276	0xccc	Not supported for classic policy.
NSERR_AS_SIG_MULTIPLE_CREDIT_CARD_RULES	3278	0xcce	Imported signatures has multiple credit card patterns in Rule.
NSERR_AS_TURNING_TAGGING_OFF_SESSIONLESS_FFC_ON	3279	0xccf	Must disable sessionless field consistency checks before disabling form tagging.
NSERR_AS_TURNING_SESSIONLESS_FFC_ON_TAGGING_OFF	3280	0xcd0	Form tagging must be enabled before enabling sessionless field consistency checks.
NSERR_AS_SIG_INVALID_CREDIT_CARD_PATTERN	3281	0xcd1	Imported Signatures has invalid Credit Card pattern.
NSERR_AS_SIG_INVALID_SAFE_OBJECT_PATTERN	3282	0xcd2	Imported Signatures has invalid Safe Object pattern.

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_AS_IMPORT_INVALID_TAR_ARCHIVE	3283	0xcd3	Imported archive is invalid. Please provide valid tar.gz archive.
NSERR_AS_SQLINJECTION_KEYWORD_INVALID_ATTRIBUTE	3284	0xcd4	Imported signatures has invalid SQL injection attributes.
NSERR_AS_SPLSTRING_INVALID_ATTRIBUTE	3285	0xcd5	Imported signatures has invalid special string attributes.
NSERR_AS_SQLINJECTION_KEYWORD_LITERAL_EXCEED_MAXLEN	3286	0xcd6	Maximum allowed length for type \"LITERAL\" for keyword is 255.
NSERR_AS_SPLSTRING_LITERAL_EXCEED_MAXLEN	3287	0xcd7	Maximum allowed length for type \"LITERAL\" for special string is 255.
NSERR_AS_XSLT_TRANFORM_LATEST	3288	0xcd8	Problem converting imported signature to the latest version. For more details see /var/log/ns.log file.
NSERR_AS_XSLT_TRANFORM_USER	3289	0xcd9	Problem converting imported signature with the given xslt file. For more details see /var/log/ns.log file.

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_AS_SIG_RESP_BODY_EXPR_ERROR	3290	0xcda	Match type EXPRESSION is not supported in response rules.
NSERR_AS_NOTRUSTEDLEARNINGCLIENT	3291	0xcdb	No Such Trusted Learning Client.
NSERR_AS_EXIST_TRUSTEDLEARNINGCLIENT	3292	0xcdc	The Trusted Learning Client is already in use.
NSERR_AS_POLICY_ALLOWED_BINDPOINT_NONE	3293	0xcdd	Only bindpoint none is allowed for this policy.
NSERR_AS_XSS_DENIED_PATTERN_INVALID_ATTRIBUTE	3294	0xcde	Imported signatures has invalid denied pattern attribute.
NSERR_AS_XSS_DENIED_PATTERN_EXCEED_MAXLEN	3295	0xcdf	Maximum allowed length for type \"LITERAL\" for denied pattern is 255.
NSERR_AS_XSS_ALLOWED_PATTERN_INVALID_ATTRIBUTE	3296	0xce0	Imported signatures has invalid allowed pattern attribute.
NSERR_AS_XSS_ALLOWED_PATTERN_EXCEED_MAXLEN	3297	0xce1	Maximum allowed length for type \"LITERAL\" for allowed pattern is 255.

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_AS_SIG_MULTIPLE_SUB_LOCATIONS	3298	0xce2	Imported signature pattern location has multiple sub locations
NSERR_AS_SIG_INTERNAL_ERROR	3299	0xce3	Internal error when configuring signatures.
NSERR_AS_SIG_URL_TAG_ERROR	3300	0xce4	Signature file has tag in an improper location.
NSERR_AS_SIG_HEADER_NAME_TAG_ERROR	3301	0xce5	Signature file has tag in an improper location. See /var/log/ns.log for more details.
NSERR_AS_SIG_COOKIE_NAME_TAG_ERROR	3302	0xce6	Signature file has tag in an improper location. See /var/log/ns.log for more details.
NSERR_AS_SIG_FIELD_NAME_TAG_ERROR	3303	0xce7	Signature file has tag in an improper location.
NSERR_AS_SIG_PATTERN_ADD_ERROR	3304	0xce8	Problem constructing signature pattern from file
NSERR_AS_SIG_NON_LITERAL_FASTMATCH	3305	0xce9	Signature file has \"fastmatch\" on a non-literal match. See /var/log/ns.log for more details

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_AS_SIG_NEGATED_LITERAL_FASTMATCH	3306	0xcea	Signature file has \"fastmatch\" on a negated literal match.
NSERR_AS_SIG_MEM_ALLOC_FAILED	3307	0xceb	Memory allocation failed while loading signatures.
NSERR_AS_SIG_TOO_MANY_PATTERNS	3308	0xcec	Signature file has a rule with too many patterns.
NSERR_AS_SIG_LITERAL_HEX_PARSE_ERROR	3309	0xced	Signature file has a pattern with hex byte syntax error.
NSERR_AS_SIG_PCRE_COMPILE_ERROR	3310	0xcee	Signature file has an invalid PCRE.
NSERR_INVALID_SIGNATURE_NAME	3311	0xcef	Invalid signature name; it must begin with an alphanumeric character or underscore and must contain only alphanumerics, '_', '.', or '-'
NSERR_AS_SIGNATURE_MERGE	3312	0xcf0	Problem merging imported signature rules with the existing signature rules. For more details see /var/log/ns.log file.

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_AS_RECORDER_MEM_ALLOC_ERROR	3313	0xcf1	Cannot allocate memory for requested recorder size.
NSERR_AS_SIG_INVALID_FILE_VERSION	3314	0xcf2	Signature file has an invalid SignaturesFile 'version' value.
NSERR_AS_AUTO_SIGNATURE_UPDATED_FAILED	3315	0xcf3	Updating of signatures failed. For more details see /var/log/ns.log file.
NSERR_AS_NO_CONTENT_TYPE	3316	0xcf4	No Such content-type.
NSERR_AS_EXIST_LOG_EXPRESSION	3317	0xcf5	LogExpression is already in use.
NSERR_AS_POLICY_SET_NOTALLOWED	3318	0xcf6	Set disallowed as advance profile can only be associated to policy that is either not bound or bound to spotted vservers.
NSERR_AS_SIGNATURE_URL_NOT_ACCESSIBLE	3319	0xcf7	Signature URL set in 'set appfw settings' is not accessible. Please check the DNS NameServer/ Route settings and try again.
NSERR_AS_NODEGROUP_UNBIND_VSERVER_NOTALLOWED	3320	0xcf8	Unbinding vserver from nodegroup disallowed as

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
			vserver has appfw policy bound to it.
NSERR_AS_NODEGROUP_BIND_NODE_NOTALLOWED	3321	0xcf9	Nodegroup could be associated with only one node if it has a vserver that has appfw policy bound to it.
NSERR_AS_BUILT_IN_OBJECT_ERROR	3322	0xcfa	Cannot add or remove built in objects.
NSERR_AS_SIGNATURE_VALIDATE_FAILED	3323	0xcfb	Imported signature is failed to validate against sha1 file. For more details see /var/log/ns.log file.
NSERR_AS_BAD_ACTION_INFER_CONTENT_TYPE_XML_PAYLOAD	3324	0xcfc	Invalid XML Infer Content-Type action.
NSERR_AS_INVALID_PARAMETER	3325	0xcfd	Sha1 parameter is allowed to use only with Import Appfw Signatures command
NSERR_AS_LEARNING_DB_ERROR	3326	0xcfe	Learning database is either corrupt or does not exist.
NSERR_AS_VALIDATION_SIGNATURE_MAPPING_FAILED	3327	0xcff	SignatureMapping.xml is invalid. Failed to validate SignatureMapping.xml against its schema file.

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_AS_EXIST_CONTENT_TYPE	3332	0xd04	Content-type is already in use.
NSERR_AS_SIG_MISSING_MAX_MATCH_LEN	3333	0xd05	Signature file has a rule with a response body pattern without the required maxMatchLength attribute
NSERR_AS_NOT_ALLOWED_CONTENT_TYPE	3334	0xd06	Content-types 'application/x-www-form-urlencoded' or 'multipart/form-data' or 'text/x-gwt-rpc' are allowed by default and do not need to be explicitly configured in the allowed list
NSERR_AS_TOTAL_IMPORT_SIZE_LIMIT_EXCEEDED	3335	0xd07	Update is successful but update operation of this import object exceeded total import size limit. Now total import size limit is changed to newer value.
NSERR_AS_MAX_TOTAL_IMPORT_LIMIT_EXCEEDED	3336	0xd08	Update operation of this import object exceeded maximum total import size limit. Please remove the object.
NSERR_INVALID_DEFAULT_SIGNATURE_NAME	3337	0xd09	Signature name must only be '*Default Signatures'

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
			or '*Xpath Injection Patterns'
NSERR_AS_SIG_OFFSET_GTE_DEPTH	3338	0xd0a	Signature file has a pattern with offset attribute greater than or equal to the depth attribute. See /var/log/ns.log for more details
NSERR_AS_SQLWILDCHAR_INVALID_ATTRIBUTE	3339	0xd0b	Imported signatures has invalid wild char attributes.
NSERR_AS_WILDCHAR_LITERAL_EXCEED_MAXLEN	3340	0xd0c	Maximum allowed length for type \"LITERAL\" for wild char exceeded.
NSERR_AS_SIG_EXCLAMATION_LITERAL	3341	0xd0d	Cannot have an exclamation point alone as a literal
NSERR_AS_REMOVE_FAILED_RENAME_FAILED	3342	0xd0e	Problem in removing resource - file rename failed
NSERR_AS_ARCHIVE_PROFILE_FAILED	3343	0xd0f	Some commands failed during archive profile. Please see /var/log/ns.log for more details.
NSERR_AS_RESTORE_PROFILE_FAILED	3345	0xd11	Some commands failed during restore profile. Please see /var/log/ns.log for more details.

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_AS_EMPTY_CONTENT_TYPE	3352	0xd18	Empty content type
NSERR_AS_SIG_FASTMATCH_BAD_LOCATION	3359	0xd1f	A signature rule has fastmatch pattern in a bad location. See log for details.
NSERR_AS_SESSIONLESS_FFC_POST_ONLY	3360	0xd20	'POST ONLY' is same as option 'ON' in streaming
NSERR_AS_TURNING_TAGGING_OFF_FFC_ON	3361	0xd21	Form-tagging cannot be disabled and remains enabled as long as field consistency check is enabled.
NSERR_AS_NO_CREDIT_CARD_NUMBER	3363	0xd23	No such credit card number.
NSERR_AS_EXIST_CREDIT_CARD_NUMBER	3364	0xd24	Credit card number is already in use.
NSERR_AS_NO_SUCH_IMPORTED_OBJECT	3365	0xd25	No such imported object.
NSERR_AS_LEARNING_SQL_ERROR	3366	0xd26	SQL Error when performing learning operation
NSERR_AS_IMPORT_FILE_IS_EMPTY	3367	0xd27	Imported file is empty
NSERR_AS_IMPORT_OVERWRITE_OP	3368	0xd28	Overwrite option is not supported.

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
TION_NOT_SUPPORTED			
NSERR_AS_BAD_INSPECT_CONTENT_TYPE	3369	0xd29	Invalid inspection content type
NSERR_AS_GEO_LOCATION_LOGGING_ENABLED	3376	0xd30	GeoLocationLogging only works when CEFLogging is enabled
NSERR_AS_NO_SUCH_WSDL_OBJECT	3377	0xd31	WSDL does not exist
NSERR_AS_NO_SUCH_XMLSCHEMA_OBJECT	3378	0xd32	XMLSchema does not exist
NSERR_AS_NO_SUCH_XMLERRORPAGE_OBJECT	3379	0xd33	XMLErrorPage does not exist
NSERR_AS_NO_SUCH_SIGNATURE_OBJECT	3380	0xd34	Signature does not exist
NSERR_AS_NO_SUCH_ARCHIVE_OBJECT	3381	0xd35	Archive does not exist
NSERR_AS_NO_SUCH_HTMLERRORPAGE_OBJECT	3382	0xd36	HTMLErrorPage does not exist
NSERR_AS_XSS_ALLOWED_TAG_INVALID_ATTRIBUTE	3393	0xd41	Xss allowed Tag has invalid attribute

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_AS_XSS_ALLOWED_ATTR_INVALID_ATTRIBUTE	3394	0xd42	Xss allowed attribute has invalid attribute
NSERR_AS_SQL_TRANSFORM_INVALID_ATTRIBUTE	3395	0xd43	SQL transform has invalid attribute
NSERR_AS_SRC_NOT_DEFAULT	3403	0xd4b	
NSERR_AS_SRC_INVALID	3404	0xd4c	Invalid source
NSERR_AS_IMPORT_NOT_DEFAULT_WITH_SHA1	3405	0xd4d	Name should be *Default Signatures when -sha1 is specified
NSERR_AS_WAR_UPDATE_FOLLOWED_BY_IMPORT	3407	0xd4f	Execute update command to push the object to packet engine so that the imported object is applied.
NSERR_AS_CUSTOM_SETTINGS_SQL_MULTIPLE_INJECTION_TYPE	3423	0xd5f	Failed to set signature object. Multiple injection tags of sql type are not allowed
NSERR_AS_BAD_CCARD_FLAGS	3439	0xd6f	Invalid Credit Card Value
NSERR_AS_NO_LOGEXPRESSION	3790	0xece	No Such Log Expression

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_AS_RFCPROFILE_BAD_ACTION	3808	0xee0	Bad rfc profile action
NSERR_AS_RFCPROFILE	3809	0xee1	Invalid rfc profile action
NSERR_AS_BAD_MALFORMED_REQ_ACTION	3814	0xee6	Invalid malformed request Action
NSERR_AS_SIG_INVALID_RULE_YEAR	3822	0xeee	Invalid year attribute value in imported signature.
NSERR_AS_SIG_INVALID_CPU_USAGE	2442	0x98A	Invalid cpu usage attribute value in imported signature.
NSERR_AS_SIG_INVALID_SEVERITY	2443	0x98B	Invalid severity attribute value in imported signature.
NSERR_AS_NO_JSON_XSS	2554	0x9fa	No such JSON XSS check
NSERR_AS_EXIST_JSON_XSS	2549	0x9f5	The JSON XSS check is already in use
NSERR_AS_NO_JSON_SQL	2553	0x9f9	No such JSON SQL check
NSERR_AS_EXIST_JSON_SQL	3582	0xdfe	The JSON SQL check is already in use
NSERR_AS_BAD_ACTION_JSON_DOS	3447	0xd77	Invalid JSON Dos Action

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_AS_EXIST_JSON_DOS_URL	3448	0xd78	The JSON DoS URL check is already in use
NSERR_AS_JSON_URL_NOT_SUPPORTED	3449	0xd79	Only .* is supported for JSON checks
NSERR_AS_NO_JSON_DOS_URL	3450	0xd7a	No such URL exist for JSON DOS check.
NSERR_AS_PROFILE_CHANGE_JSON	3451	0xd7b	JSON checks will not be applicable when profile type is not JSON
NSERR_AS_BAD_ACTION_JSON_SQL	3452	0xd7c	Invalid JSON SQLInjection Action
NSERR_AS_BAD_ACTION_JSON_XSS	3453	0xd7d	Invalid JSON CrossSiteScripting Action
NSERR_AS_NO_SUCH_JSONERRORPAGE_OBJECT	3501	0xdad	JSONErrorPage does not exist
NSERR_AS_PROFILE_CHANGE_HTML_JSON	3500	0xdac	HTML, JSON checks will not be applicable when profile type is not HTML or JSON respectively
NSERR_AS_PROFILE_CHANGE_HTML_XML	3502	0xdae	HTML, XML checks will not be applicable when profile type is not HTML or XML respectively

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_AS_PROFILE_CHANGE_XML_JSON	3503	0xdaf	XML, JSON checks will not be applicable when profile type is not XML or JSON respectively
NSERR_AS_PROFILE_CHANGE_HTML_XML_JSON	3488	0xda0	HTML, XML, JSON checks will not be applicable when profile type is not HTML, XML or JSON respectively
NSERR_AS_NO_FILEUPLOAD_TYPE	3848	0xf08	No Such File Upload Type.
NSERR_AS_BAD_ACTION_FILEUPLOAD_TYPE	361	0x169	Invalid File Upload Types Action
NSERR_AS_DYNAMIC_PROFILING_NOT_SUPPORTED	3849	0xf09	Dynamic Profiling is not supported in cluster mode
NSERR_AS_BAD_ACTION_DYNAMIC_PROFILING	3850	0xf0a	Invalid Dynamic Profiling Action.
NSERR_AS_INVALID_RESTORE_PROFILE	385	0x181	Invalid Restore operation. Relaxation rules not enabled for restore.
NSERR_AS_INVALID_RESTORE_PROFILE_ACTION	386	0x182	Invalid Restore operation. Overwrite and Augment can't both be specified.

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_AS_INVALID_RESTORE_PROFILE_URL	387	0x183	Invalid Restore operation. Match URL and Replace URL must both be specified if either one is present.
NSERR_AS_BAD_ACTION_COOKIE_HIJACKING	388	0x184	Invalid Cookie Hijacking Action
NSERR_AS_SNORT_CONVERT	4051	0xfd3	Problem converting snort rules to WAF signature file. For more details see /var/log/ns.log file.
NSERR_AS_CMDINJECTION_KEYWORD_INVALID_ATTRIBUTE	3245	0xcad	Imported signature has invalid Command injection attributes.
NSERR_AS_CMD_NOT_EXIST	2986	0xbaa	Specified command injection relaxation rule does not exist
NSERR_AS_PART_DIR_NOT_FOUND	3007	0xbbf	Error in getting partition specific directory.
NSERR_AS_FAKEACCOUNT	390	0x186	Fake Account Error
NSERR_AS_CFFIELD	391	0x187	Confidential Field Error
NSERR_AS_BLOCKKEYWORD	392	0x188	Block Keyword Error

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_AS_JSON_BLOCKKEYWORD	393	0x189	JSON Block Keyword Error
NSERR_AS_BYPASS_LIST	3851	0xf0b	Bypass List Error
NSERR_AS_DENY_LIST	3852	0xf0c	Deny List Error

BACKUP ERRORS

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_BACKUP_CONFINVALID	3425	0xd61	Configuration file is not valid or corrupted.
NSERR_BACKUP_CREATEDIR	3426	0xd62	Unable to create directory .
NSERR_BACKUP_MISSING	3427	0xd63	Backup file does not exist.
NSERR_BACKUP_CREATETAR	3428	0xd64	Unable to create backup tar file.
NSERR_BACKUP_CONFMISSING	3429	0xd65	Configuration file not found.
NSERR_BACKUP_FILEMISSING	3430	0xd66	Missing filename argument in the input.
NSERR_BACKUP_INVALIDFILE	3431	0xd67	Invalid/Tampered backup file encountered.
NSERR_BACKUP_EXTRACTTAR	3432	0xd68	Unable to extract backup tar file.

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_BACKUP_REMOVE	3433	0xd69	Unable to remove backup tar file.
NSERR_BACKUP_MAXLIMIT	3434	0xd6a	Reached max limit of 50 for backup files. Remove older files to proceed.

BASE ERRORS

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_NOTRUNNING	256	0x100	NetScaler not running
NSERR_PERM	257	0x101	Operation not permitted
NSERR_NOENT	258	0x102	No such resource
NSERR_SRCH	259	0x103	No such process
NSERR_INTR	260	0x104	Interrupted system call
NSERR_IO	261	0x105	Input/output error
NSERR_NXIO	262	0x106	Device not configured
NSERR_2BIG	263	0x107	Argument list too long
NSERR_NOEXEC	264	0x108	Exec format error
NSERR_BADF	265	0x109	Bad file descriptor
NSERR_CHILD	266	0x10A	No child processes

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_DEADLK	267	0x10B	Resource deadlock avoided
NSERR_NOMEM	268	0x10C	Cannot allocate memory
NSERR_ACCES	269	0x10D	Permission denied
NSERR_FAULT	270	0x10E	Bad address
NSERR_NOTBLK	271	0x10F	Block device required
NSERR_BUSY	272	0x110	Device busy
NSERR_EXIST	273	0x111	Resource already exists
NSERR_XDEV	274	0x112	Cross-device link
NSERR_NODEV	275	0x113	Operation not supported by device
NSERR_NOTDIR	276	0x114	Not a directory
NSERR_ISDIR	277	0x115	Is a directory
NSERR_INVAL	278	0x116	Invalid argument
NSERR_NFILE	279	0x117	Too many open files in system
NSERR_MFILE	280	0x118	Too many open files
NSERR_NOTTY	281	0x119	Inappropriate ioctl for device
NSERR_TXTBSY	282	0x11A	Text file busy
NSERR_FBIG	283	0x11B	File too large

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_NOSPACE	284	0x11C	No space left on device
NSERR_SPIPE	285	0x11D	Illegal seek
NSERR_ROFS	286	0x11E	Read-only file system
NSERR_MLINK	287	0x11F	Too many links
NSERR_PIPE	288	0x120	Broken pipe
NSERR_DOM	289	0x121	Numerical argument out of domain
NSERR_RANGE	290	0x122	Result too large
NSERR_AGAIN	291	0x123	Resource temporarily unavailable
NSERR_INPROGRESS	292	0x124	Operation now in progress
NSERR_ALREADY	293	0x125	Operation already in progress
NSERR_NOTSOCK	294	0x126	Socket operation on non-socket
NSERR_DESTADDRREQ	295	0x127	Destination address required
NSERR_MSGSIZE	296	0x128	Message too long
NSERR_PROTOTYPE	297	0x129	Protocol wrong type for socket
NSERR_NOPROTOOPT	298	0x12A	Protocol not available

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_PROTONOSUPPORT	299	0x12B	Protocol not supported
NSERR_SOCKTNOSUPPORT	300	0x12C	Socket type not supported
NSERR_OPNOTSUPP	301	0x12D	Operation not supported
NSERR_PFNOSUPPORT	302	0x12E	Protocol family not supported
NSERR_AFNOSUPPORT	303	0x12F	Address family not supported by protocol family
NSERR_ADDRINUSE	304	0x130	Address already in use
NSERR_ADDRNOTAVAIL	305	0x131	Can't assign requested address
NSERR_NETDOWN	306	0x132	Network is down
NSERR_NETUNREACH	307	0x133	Network is unreachable
NSERR_NETRESET	308	0x134	Network dropped connection on reset
NSERR_CONNABORTED	309	0x135	Software caused connection abort
NSERR_CONNRESET	310	0x136	Connection reset by peer
NSERR_NOBUFS	311	0x137	No buffer space available
NSERR_ISCONN	312	0x138	Socket is already connected

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_NOTCONN	313	0x139	Socket is not connected
NSERR_SHUTDOWN	314	0x13A	Can't send after socket shutdown
NSERR_TOOMANYREFS	315	0x13B	Resource in use
NSERR_TIMEDOUT	316	0x13C	Operation timed out
NSERR_CONNREFUSED	317	0x13D	Connection refused
NSERR_LOOP	318	0x13E	Too many levels of symbolic links
NSERR_NAMETOOLONG	319	0x13F	File name too long
NSERR_HOSTDOWN	320	0x140	Host is down
NSERR_HOSTUNREACH	321	0x141	No route to host
NSERR_NOTEMPTY	322	0x142	Directory not empty
NSERR_PROCLIM	323	0x143	Too many processes
NSERR_USERS	324	0x144	Too many users
NSERR_DQUOT	325	0x145	Disc quota exceeded
NSERR_STALE	326	0x146	Stale NFS file handle
NSERR_REMOTE	327	0x147	Too many levels of remote in path
NSERR_BADRPC	328	0x148	RPC struct is bad

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_RPCMISMATCH	329	0x149	RPC version wrong
NSERR_PROGUNAVAIL	330	0x14A	RPC prog. not avail
NSERR_PROGMISMATCH	331	0x14B	Program version wrong
NSERR_PROCUNAVAIL	332	0x14C	Bad procedure for program
NSERR_NOLCK	333	0x14D	No locks available
NSERR_NOSYS	334	0x14E	System Call not supported; Possible Reason: NetScaler is not running
NSERR_FTYPE	335	0x14F	Inappropriate file type or format
NSERR_AUTH	336	0x150	Authentication error
NSERR_NEEDAUTH	337	0x151	Need authenticator
NSERR_WOULDBLOCK	338	0x152	Operation would block
NSERR_NOCODE	339	0x153	Feature is not implemented
NSERR_NOTSUSER	340	0x154	Not super-user
NSERR_BIGDATA	341	0x155	Data size is too big
NSERR_SMALLDATA	342	0x156	Data size is too small

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_NOMORENT	343	0x157	No more entry in table
NSERR_NOSERVICE	344	0x158	No Service
NSERR_OSERROR	345	0x159	Operating system error
NSERR_NONEXPCMD	346	0x15A	Unexpected command
NSERR_CMDPROPFAIL	347	0x15B	Command propagation failed
NSERR_TOOMANYNODES	348	0x15C	Too many nodes
NSERR_SECONDARYFAIL	349	0x15D	Command failed on secondary node, but succeeded on primary node. Configuration will be synchronized to ensure secondary and primary have same configuration.
NSERR_INVALBACKUP	350	0x15E	Invalid backup vserver
NSERR_NOSERVER	351	0x15F	No such server
NSERR_LOGINREQD	352	0x160	Login is required
NSERR_RPCINVAL	353	0x161	RPC invalid argument

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_NOUSER	354	0x162	Invalid username or password
NSERR_INVALPASSWD	355	0x163	Invalid username or password
NSERR_PASSWORD_EXPIRED_CHANGEPWD	400	0x190	Password has expired. Please login from CLI/GUI to change the password
NSERR_LICENSE	356	0x164	Feature(s) not licensed
NSERR_DEFERRED	357	0x165	The command is stored for later execution
NSERR_PROPAUTHFAIL	358	0x166	Command propagation failed due to user authentication problems
NSERR_NODELSUSER	359	0x167	The superuser cannot be removed
NSERR_NOMODSUSER	360	0x168	Permissions for this superuser cannot be modified
NSERR_INVALNODEID	362	0x16A	Invalid node ID specified
NSERR_NOTOPHA	363	0x16B	Operation not permitted on stand-alone node

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_NOOPPEERBAD	364	0x16c	Operation not possible due to invalid peer state. Rectify and retry.
NSERR_NOOPBAD	365	0x16d	Operation not possible as system state is invalid. Use show node for more information.
NSERR_NOPNOW	366	0x16e	Operation not possible now. Please wait for system to stabilize before retrying.
NSERR_NOOPPRI	367	0x16f	Operation permitted only on secondary node.
NSERR_NOOPSEC	368	0x170	Operation permitted only on primary node.
NSERR_REDIRECT	369	0x171	Redirect request (VIP down)
NSERR_BUFOVERFLOW	370	0x172	Buffer overflow occurred
NSERR_NOUSERPOLICY	371	0x173	No command policy defined, permission denied
NSERR_NOSYSGROUP	372	0x174	System group does not exist
NSERR_NOSYSCMDPOL	373	0x175	System command policy does not exist

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_HAIPV6PT	374	0x176	IPV6 Feature cannot be disabled while HA is running over IPv6.
NSERR_HANSIPV6	375	0x177	IPv6 NSIP cannot be changed while HA is running over IPv6.
NSERR_NSIPV6ACTIVE	376	0x178	IPv6 NSIP is not in ACTIVE state, rectify and retry.
NSERR_RTMON_STANDALONE	377	0x179	Unbind all route monitors before making node standalone.
NSERR_INTERFACENOTALLOWED	384	0x180	Unauthorized: User is not allowed through this interface
NSERR_IPV6FEAT_DISABLED	378	0x17a	IPv6 Feature Disabled
NSERR_DHCP_PBR_DEPENDENT	379	0x17b	PBR rule present with nexthop dependent on released DHCP lease
NSERR_IPSECPROF_PERM	380	0x17c	Tunnel protocol IPSEC must have ipsec profile set to 'none'.
NSERR_IFPAIR_BOUND	381	0x17d	Interface(s) already member of other interface pair

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_IFPAIR_NOTPAIR	382	0x17e	Number of member interfaces need to be exactly 2
NSERR_PBR_SETIPTUNNEL	383	0x17f	SET operations on PBR for changing iptunnel not allowed. Remove and add PBR with new iptunnel
NSERR_IPRANGENOTALLOWD	394	0x18A	Range not allowed for wildcard IP
NSERR_IVALIDIPRANGE	395	0x18B	Invalid range value
NSERR_IPRANGEMAXLIMIT	396	0x18C	Range value greater than maximum limit 254
NSERR_IP_NOT_EXIST	397	0x18D	IP does not exist for default or specified td
NSERR_TOOMANYRULES	398	0x18E	Maximum number of ACLs on the system has been exceeded
NSERR_PASSWD_LEN_MIN_8	399	0x18F	Password too short - minimum length is 8 characters
NSERR_SYNC_DISABLED	410	0x19A	Synchronization disabled
NSERR_NODE_DISABLED	411	0x19B	Node disabled

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_SYNC_PROGRESS	412	0x19C	Synchronization is in progress
NSERR_ADNS_PERM	413	0x19D	Operation not permitted on ADNS service
NSERR_NOINC_IPSAMESUBNET	414	0x19E	Peer IP should be on the NSIP subnet if INC mode is disabled
NSERR_INVALID_PEERIP	415	0x19F	Not a valid peer IP
NSERR_REDIRECT307	416	0x1A0	Redirect request (send 307 temporary redirect
NSERR_INVALHOSTNAME	417	0x1A1	Invalid hostname
NSERR_REWRITE_NOT_SUPPORTED	418	0x1A2	Port rewrite not supported on this vserver type
NSERR_IPCHG_DENY	419	0x1A3	IP address change not permitted on this entity
NSERR_IPCHG_GSLB	420	0x1A4	GSLB local service IP cannot be changed. Please change the corresponding vserver's IP
NSERR_GSLB_IPCHG	421	0x1A5	corresponding GSLB service/GSLB

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
			service item IP has also been changed.
NSERR_NOAUDITSRVC	422	0x1A6	No audit service running on the specified port
NSERR_LACPKEY_NOTSET	423	0x1A7	LACP key not set
NSERR_CHANNEL_INUSEBYLACP	424	0x1A8	Channel in use by LACP
NSERR_LACPENABLED	425	0x1A9	LACP enabled interface cannot be bound manually to a channel
NSERR_IFACEMANUALLYBOUND	426	0x1AA	LACP cannot be enabled, interface manually bound to a channel
NSERR_INTRECINUSE	427	0x1AB	Domain name for the reverse domain name already exists
NSERR_PUBIPPORT_VIP_CONFLICT	428	0x1AC	Public IP, port conflict with another entity bound to the same GSLB vserver
NSERR_IPPORT_VIP_BOUND	429	0x1AD	IP, port conflict with an entity already bound to the vserver
NSERR_NO_BACKUP_VIP	430	0x1AE	No such backup vserver
NSERR_REQ_SET_ARGS	431	0x1AF	No arguments to set

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_SVCGRP_MEMBER_NAMECONFLICT	432	0x1B0	Name conflicts with an existing service or service group member name
NSERR_SERVER_NAME_EXIST	433	0x1B1	Server name already exists
NSERR_MAX_SERVICE_BINDING_ON_VSERVER	434	0x1B2	Maximum services bound to vserver exceeded
NSERR_MAX_SVC_ENTITY_BINDING_ON_SVCGROUP	435	0x1B3	Maximum services bound to service group exceeded
NSERR_FSMALL	436	0x1B4	File too small
NSERR_INTOFLOW	437	0x1B5	Integer overflow
NSERR_ASYNC_BLOCKED	438	0x1B6	Expression evaluation has blocked for body accumulation
NSERR_SACL_CLEARPENDING	439	0x1B7	Clear in progress
NSERR_SACL_NAME_EXISTS	440	0x1B8	An ACL with the same name exists
NSERR_SACL_SUPERSET_EXISTS	441	0x1B9	Operation not permitted. (An overlapping rule already exists)
NSERR_SACL_SUBSET_EXISTS	442	0x1BA	Operation not permitted. (A rule which is subset of

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
			this rule already exists)
NSERR_NOINC_ROUTEMONITOR	443	0x1BB	Route monitors should be added only if INC mode is enabled
NSERR_SESSION_EXPIRED	444	0x1BC	Session expired or killed. Please login again
NSERR_SESSION_EXCEEDED	445	0x1BD	Session limit exceeded
NSERR_CFE_CONN_EXCEEDED	446	0x1BE	Connection limit to CFE exceeded
NSERR_CFE_KILLSELF	449	0x1C1	Invalid session id. Current session cannot be killed
NSERR_CFE_INCOMPLETESESSION	450	0x1C2	Invalid session. Response/challenge is incomplete
NSERR_ACL_ALREADYINSTATE	451	0x1C3	Entity already in this state
NSERR_CFE_SESSION_NOEXIST	452	0x1C4	Session does not exist
NSERR_SYSGROUP_USER_EXISTS	453	0x1C5	User already bound to system group
NSERR_SYSGROUP_POLICY_EXISTS	454	0x1C6	Policy already bound to system group
NSERR_SLEEP	455	0x1C7	Sleep process sleep
NSERR_PPEDIE	456	0x1C8	Your PPE is no more

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_NOCONN_CMDPROPFAIL	457	0x1C9	Unable to establish connection with the secondary. Command propagation failed
NSERR_TIMEOUT_SECONDARY	458	0x1CA	There is no response from the secondary. Propagation timed out
NSERR_RPC_TIMEOUT	459	0x1CB	RPC timeout
NSERR_NOT_SUPPORTED	460	0x1CC	Feature not supported in this release
NSERR_NOENT_VSERVER	461	0x1CD	No such Vserver
NSERR_NOENT_SVC	462	0x1CE	No such service
NSERR_NOENT_SVC_SVCGRP	463	0x1CF	No such service/ serviceGroup
NSERR_HA_NOV4_NETMASK	464	0x1D0	IPv4 netmask is not required for IPv6
NSERR_MAX_VSEVRVER_BINDINGS_TO_SERVICE	465	0x1D1	Maximum vservers bound to a service exceeded
NSERR_SACL6_CLEARPENDING	466	0x1D2	Simple ACL6 Clear in progress
NSERR_SACL6_NAME_EXISTS	467	0x1D3	Simple ACL6 with the same name exists

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_SACL6_SUPERSET_EXISTS	468	0x1D4	Operation not permitted. (An overlapping rule already exists)
NSERR_SACL6_SUBSET_EXISTS	469	0x1D5	Operation not permitted. (A rule which is subset of this rule already exists)
NSERR_NO_BACKUP_VIP_BOUND	470	0x1D6	No backupVserver bound
NSERR_SESSION_EXPIRED_REDIRECT	471	0x1D7	Session expired, Please login again
NSERR_NOENT_VLAN	472	0x1D8	Vlan does not exist
NSERR_MAX_SVC_ENTITY	473	0x1D9	Maximum service limit reached
NSERR_CL_EXIST	474	0x1DA	Resource already exists in cluster
NSERR_OWNERNODE_NOTALLOWED	475	0x1DB	Can not specify owner node.
NSERR_OWNERNODE_NOT_SPECIFIED	476	0x1DC	Owner node is not specified.
NSERR_NOT_SUPPINCLUSTER	477	0x1DD	Operation not supported in Cluster.
NSERR_VSERVER_TYPE_MISMATCH	478	0x1DE	Vserver type mismatch.

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_ITER_END	479	0x1DF	End of iteration reached.
NSERR_CONNECT_TO_CLUSTER_IP	1382	0x566	Please connect to cluster IP and run showtechsupport on that node.
NSERR_LB_AUDIT_IP_DENY	1383	0x567	Changing IP address of LB vserver not permitted when Audit server also referring to same server_info .
NSERR_IC_OFF_DISABLING_FEO	1384	0x568	IC is disabled, but FEO is enabled.
NSERR_SYNC_VLAN_EXIST	1385	0x569	Please unset sync vlan, before removing the HA node.
NSERR_CMDPROP_DISABLED	1450	0x5AA	Command propagation disabled.
NSERR_NOTHEME	1451	0x5AB	Portal theme doesn't exist
NSERR_THEMEEXISTS	1452	0x5AC	Portal theme already exists
NSERR_THEME_INUSE	1453	0x5AD	Portal theme in use
NSERR_NO_CONTENT	1454	0x5AE	204 No Content

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_ARP_IFACE_NODE_MISMATCH	1440	0x5a0	Interface and node mismatch
NSERR_HA_BOTH_PRIMARY	1441	0x5a1	Cannot failover as Node State set to STAYPRIMARY
NSERR_PROP_DISABLED	1448	0x5a8	Propagation disabled
NSERR_HA_FAILOVER_PERM	1449	0x5a9	Failover not permitted as one node is up and another node is down
NSERR_NOEULA	938	0x3AA	Eula name doesn't exist
NSERR_EULAEXISTS	939	0x3AB	Eula with same name already exists
NSERR_EULA_INUSE	940	0x3AC	Eula name in use
NSERR_SYSLOG_TCP_CONFIG_ERR	1459	0x5B3	tcpProfileName/ maxLogDataSizeToHold cannot be set when transport is UDP
NSERR_SYSLOG_LOOPBACK_OR_LOCAL_IP_NOTALLOWED	1460	0x5B4	TCP transport is not allowed for local logging(when serverIP is configured as Loopback IP or NetScaler's local IP)

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_MAX_CONC_SAVECONFIG	1461	0x5B5	Maximum number of concurrent save configs are in progress. Try again later.
NSERR_SYSLOG_LBMETHOD_NOTALLOWED	1462	0x5B6	LB method AUDITLOGHASH can be set only for service type SYSLOGTCP/ SYSLOGUDP
NSERR_SYSLOG_PERSISTENCE_NOTSUPPORTED	1463	0x5B7	Persistency is not supported for SYSLOGTCP and SYSLOGUDP service types
NSERR_SYSLOG_HASHLBMETHODS_NOTALLOWED	1464	0x5B8	Hash based LB methods which depend on packet parameters cannot be set for SYSLOGTCP/ SYSLOGUDP service types
NSERR_SYSLOG_LEASTCONN_NOTSUPPORTED	1467	0x5BB	LEASTCONNECTION algorithm is not supported for SYSLOGTCP/ SYSLOGUDP service types
NSERR_SVC_EXISTS	1468	0x5BC	Service exists with this server information

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_SYSLOG_NOLBVIP	1469	0x5BD	No such LB vserver of type SYSLOGUDP/ SYSLOGTCP exists
NSERR_SYSLOG_LBPROTOCOL_NOTALLOWED	1470	0x5BE	LB vserver of type other than SYSLOGUDP/ SYSLOGTCP/HTTP cannot be set to syslogaction
NSERR_SYSLOG_TRANSPORT_UNSET_NOTALLOWED	1471	0x5BF	Transport cannot be unset when LB vserver name is configured
NSERR_SYSLOG_TRANSPORT_MISMATCH	1472	0x5C0	Mismatch in transport type of LB vserver and syslog action
NSERR_SYSLOG_LBVSRVR_INUSE_BY_SYSACT	1473	0x5C1	The LB vserver is being accessed by syslog action
NSERR_SYSLOG_LBVSRVR_RENAME_NOTSUPPORTED	1474	0x5C2	Renaming LB vserver is not supported for SYSLOGUDP/ SYSLOGTCP service types
NSERR_SYSLOG_INVALID_SERVIP	1475	0x5C3	ServerIP cannot be configured as 0.0.0.0 or 0 for syslog action
NSERR_AUDITLOG_PORT_SET_UNSET_NOTALLOWED	1476	0x5C4	Port cannot be set/ unset when LB vserver name/Server

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
			domain name is configured
NSERR_SYSLOG_TCPPROFILE_NOTALLOWED	1477	0x5C5	TCP profile name cannot be set when LB vserver name is configured
NSERR_SYSLOG_CANNOT_SET_LBVSNAME	1478	0x5C6	Unset the TCP profile name and then set the LB vserver name
NSERR_MPTCP_CANNOT_SET_MPTCPADVERTISE	1495	0x5D7	MPTCP Advertise can be set only on the IP of type VIP.
NSERR_PORTALBINDING_NOT_SUPPORTED	1479	0x5C7	Operation not supported. Unset VPN uitheme parameter first and then try again.
NSERR_PORTALTHEME_NAME_NOT_ALLOWED	1480	0x5C8	\'EULA\' and \'Custom\' keywords are reserved. Please try with any other name
NSERR_AUDIT_VERSION_MISMATCH	1481	0x5C9	Audit version mismatch
NSERR_RADIUS_LISTENER_PERM	1482	0x5CA	Operation not permitted on RADIUS LISTENER service
NSERR_SYSLOG_NETPROFILE_NOTALLOWED	1483	0x5CB	Network profile name cannot be set when LB vserver name is configured

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_AUDITLOG_DMNRESOLVRETRY	1484	0x5CC	Domain name can be resolved only when server domain name is configured
NSERR_AUDITLOG_ARGUMENT_MISSING	1485	0x5CD	One of the arguments \"Server IP/Server domain name/LB vserver name\" is required for auditlog action
NSERR_AUDITLOG_DBS_SERVER_EXIST	1486	0x5CE	Auditlog internal DBS server with the same domain name exists
NSERR_ICAMODE_STATUS_NOT_OK	1487	0x5CF	vpn icamode status not okay
NSERR_SYSLOG_LBVSERVER_NOTALLOWED	1488	0x5D0	LB vserver name cannot be set when network profile is configured. Unset the netProfile and set LB vserver name
NSERR_INSTALL_FAILED	1490	0x5D2	Installation failed.
NSERR_OSPFAREA_UNSET	1491	0x5D3	Unset of OSPFArea is allowed only for VIP and SNIP
NSERR_PREQ_HOSTROUTE	1492	0x5D4	Pre-requisite Hostroute is disabled
NSERR_PREQ_NETWORKROUTE	1493	0x5D5	Pre-requisite Networkroute is disabled

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_AUDITLOG_SVC_EXISTS	1496	0x5D8	Auditlog service exists with this server information
NSERR_AUDITSINFO_EXISTS_WITH_SAME_DOMAINNAME	1497	0x5D9	Auditlog action exists with the same domain name
NSERR_INSTALL_PRE_CHECK_NOT_SUPPORTED	1498	0x5DA	Install pre-check option is not supported for the specified build
NSERR_NO_PERM_ON_PLATFORM	1501	0x5DD	Operation not supported on this platform
NSERR_NOTDBS_SERVER_AUTOSCALE_SGRP	3779	0xEC3	Cannot configure autoScale as POLICY option for an IP based server.
NSERR_AUTO_SCALE_CLOUD_API_TYPE_ONLY	3810	0xEE2	Operation is supported for servicegroup with autoscale type CLOUD or API only.
NSERR_AUTO_DISABLE_GRACEFUL_NOT_SET	3811	0xEE3	Auto Disable Graceful not enabled. Set autoDisablegraceful parameter to YES.
NSERR_AUTO_DISABLE_GRACEFUL_NOT_SUPPORTED_ON_AZURE	3812	0xEE4	Auto Disable Graceful not supported on Azure Platform.

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_MAX_MONITORS_BINDINGS_TO_SERVICE	3813	0xEE5	Maximum monitors bound to this entity exceeded
NSERR_INSUFFICIENT_IAM_PRIVILEGES	3815	0xEE7	Insufficient iam privileges configured for this feature
NSERR_LOGIN_NEXTFACTOR	3816	0xEE8	Nextfactor Login
NSERR_SVC_GRP	1855	0x73F	Unable to discover Autoscale group/ setting in cloud
NSERR_MISSING_POLICY	2197	0x895	Unable to discover scale down policy of Autoscale group/ setting in cloud
NSERR_AZURE_MANAGED_IDENTITY_NOT_ALLOWED	1508	0x5e4	The name MANAGED_IDENTITY cannot be configured in azure application. Instead, it has to be configured as azureApplication directly in azurekeyVault configuration
NSERR_AUTO_SCALE_DNS_TROFS_DELAY	1509	0x5e5	Operation is supported for servicegroup with autoscale type DNS only.
NSERR_DOH_HTTP2_REQUIRED	1510	0x5e6	To enable DOH, the attached HTTP

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
			profile must have HTTP2 enabled.
NSERR_HIT_MX_LIMIT_OF_HTTP_TRANS_SYS_ACT	1511	0x5e7	Hit the max limit for HTTP transport based syslog action(NS_AUDITLOG_MAX_ACTIONS_WITH_HTTP_TRANSPORT).
NSERR_SYSLOG_NETPROFILE_SET_NOTALLOWED	1512	0x5e8	Netfrofile can't be set/unset when Secure Mangement is enabled
NSERR_AUDIT_PLANE_MISMATCH	1513	0x5e9	Invalid traffic plane
NSERR_UNSUPPORTED_DISK_ENCRYPTION	1519	0x5EF	Unsupported operation. Platform conversion required prior to disk encryption/ decryption.
NSERR_KAFKASVC	1520	0x5f0	Kafka Broker servicegroup type Bootstrap or Topic not set.
NSERR_KAFKABIND	1521	0x5f1	Invalid kafka bind/ unbind operation.
NSERR_NO_SUCH_KAFKACLUSTER	1522	0x5f2	Kafka cluster not found.

BOT ERRORS

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_BOT_UPDATE_FAILED	1696	0x6a0	Updating the resource failed
NSERR_BOT_CFG_INVALID_JSON	1697	0x6a1	Invalid JSON Configuration
NSERR_BOT_CFG_IPREP_INVALID_CATEGORY	1713	0x6b1	Invalid category in IPReputation config
NSERR_BOT_CFG_RATELIMIT_NO_URL	1723	0x6bb	No URL option in RateLimit configuration
NSERR_BOT_CFG_RATELIMIT_NO_COOKIE	1724	0x6bc	No Cookie option in RateLimit configuration
NSERR_BOT_CFG_MAX_KM_LIMIT_REACHED	1725	0x6bd	Keyboard-mouse Config Limit exceeded.
NSERR_BOT_CFG_RATELIMIT_INVALID_CATEGORY	1726	0x6be	Invalid category in ratelimit config
NSERR_BOT_CFG_MAX_WHITELIST_LIMT_REACHED	1760	0x6e0	White List Config Limit exceeded.
NSERR_BOT_CFG_MAX_BLACKLIST_LIMT_REACHED	1761	0x6e1	Black List Config Limit exceeded.
NSERR_BOT_CFG_MAX_RATELIMIT_LIMT_REACHED	1763	0x6e3	RateLimit Config Limit exceeded.

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_BOT_SIGNATURE_URL_NOT_ACCESSIBLE	1768	0x6e8	Signature URL set in 'set bot settings' is not accessible. Please check the DNS NameServer/ Route settings and try again.
NSERR_BOT_CFG_MAX_CAPTCHA_LIMIT_REACHED	1769	0x6e9	Captcha Config Limit Exceeded
NSERR_BOT_SIGNATURE_AUTO_UPDATE_IPV6_NOT_SUPPORTED	1770	0x6ea	IPV6 is not supported.
NSERR_BOT_SIGNATURE_AUTO_UPDATE_PARSE_ERROR	1771	0x6eb	Signature Parse error
NSERR_BOT_SIGNATURE_INVALID_URL	1772	0x6ec	Invalid Signature URL.
NSERR_BOT_BAD_TRAPURL	1773	0x6ed	Invalid TrapURL. Url should start with '/'
NSERR_BOT_DEFAULT_SIGNATURE_FILE_PARSE_ERROR	1774	0x6ee	Unable to parse Bot Signature File.
NSERR_BOT_NEG_TRAP_URL_REGEX	1775	0x6ef	Negated regex are not allowed.
NSERR_BOT_INVALID_DFP_MOBILE_TYPE	1698	0x6a2	Invalid Device Fingerprint mobile type

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_BOT_UPDATE_SIGNATURE_META_UPDATE_FAILED	1701	0x6a5	Signature Auto Update meta file update failed.
NSERR_BOT_PROFILE_BINDING_ALREADY_EXISTS	1703	0x6a7	An entity with the name already bound.
NSERR_BOT_CFG_MAX_TRAPURL_LIMIT_REACHED	1702	0x6a6	Trap URL Config Limit exceeded.
NSERR_BOT_CFG_MAX_LOGEXPRESSION_LIMT_REACHED	1705	0x6a9	Log Expression Config Limit exceeded.

CACONF ERRORS

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_CACONF_CNFL_HEUREXP_RELEXP	480	0x1E0	Conflicting arguments, heurExpiryParam and relExpiry
NSERR_CACONF_CNFL_HEUREXP_RELEXPMILI	481	0x1E1	Conflicting arguments, heurExpiryParam and relExpiryMilliSec
NSERR_CACONF_CNFL_RELEXP_RELEXPMILI	482	0x1E2	Conflicting arguments, relExpiry and relExpiryMiliSec
NSERR_CACONF_CNFL_ABSEXP_HEUREXP	483	0x1E3	Conflicting arguments,

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
			absExpiry and heurExpiryParam
NSERR_CACONF_CNFL_ABSEXP_RELEXPMILI	484	0x1E4	Conflicting arguments, absExpiry and relExpiryMilliSec
NSERR_CACONF_CNFL_ABSEXPGMT_HERUEXP	485	0x1E5	Conflicting arguments, absExpiryGMT and heurExpiryParam
NSERR_CACONF_CNFL_ABSEXP_ABSEXPGMT	486	0x1E6	Conflicting arguments, absExpiry and absExpiryGMT
NSERR_CACONF_CNFL_ABSEXPGMT_RELEXPMILI	487	0x1E7	Conflicting arguments, absExpiryGMT and relExpiryMilliSec
NSERR_CACONF_CNFL_HITPARAMS_HITSLCTR	488	0x1E8	Conflicting arguments, hitParams and hitSelector
NSERR_CACONF_CNFL_INVALPARAMS_HITSLCTR	489	0x1E9	Conflicting arguments, invalParams and hitSelector
NSERR_CACONF_CNFL_HITPARAMS_INVLSLCTR	490	0x1EA	Conflicting arguments, hitParams and invalSelector
NSERR_CACONF_CNFL_INVALPARAMS_INVLSLCTR	491	0x1EB	Conflicting arguments,

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
			invalParams and invalSelector
NSERR_CACONF_CNFL_HITSLCTR_MATCHCOOKY	492	0x1EC	Conflicting arguments, hitSelector and matchCookies
NSERR_CACONF_CNFL_HITSLCTR_INVALREST2HOST	493	0x1ED	Conflicting arguments, hitSelector and invalRestrictedToHost
NSERR_CACONF_CNFL_HITSLCTR_IGNRPARAMVALCASE	494	0x1EE	Conflicting arguments, hitSelector and ignoreParamValueCase
NSERR_CACONF_CNFL_INVALSLCTR_MATCHCOOKY	495	0x1EF	Conflicting arguments, invalSelector and matchCookies
NSERR_CACONF_CNFL_INVALSLCTR_INVALREST2HOST	496	0x1F0	Conflicting arguments, invalSelector and invalRestrictedToHost
NSERR_CACONF_CNFL_INVALSLCTR_IGNRPARAMVALCASE	497	0x1F1	Conflicting arguments, invalSelector and ignoreParamValueCase
NSERR_CACONF_CNFL_POSRELEXP_RELEXP	498	0x1F2	Conflicting arguments,

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
			weekPosRelExpiry and relExpiry
NSERR_CACONF_CNFL_POSRELEXP_RELEXPMILI	499	0x1F3	Conflicting arguments, weekPosRelExpiry and relExpiryMiliSec
NSERR_CACONF_CNFL_ABSEXP_POSRELEXP	500	0x1F4	Conflicting arguments, absExpiry and weekPosRelExpiry
NSERR_CACONF_CNFL_ABSEXPGMT_POSRELEXP	501	0x1F5	Conflicting arguments, absExpiryGMT and weekPosRelExpiry
NSERR_CACONF_CNFL_IGNRPARAMVALCASE_HITPARAMS	502	0x1F6	Invalid arguments, ignoreParamValueCase is set while hitParams is 0
NSERR_CACONF_CNFL_HIT_INVALPARAMS_MATCHCUKY	503	0x1F7	Invalid arguments, matchCookies is set while both hitParams and invalParams are 0
NSERR_CACONF_CNFL_INVALREST2HOST_INVALPARAM	504	0x1F8	Invalid arguments, invalRestrictedToHost is set while invalParams is 0
NSERR_CACONF_CNFL_PREFETCH_PREFETCHSEC	505	0x1F9	Invalid arguments, prefetchPeriod is set while prefetch is disabled

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_CACONF_CNFL_PREFETCH_PREFETCHMILI	506	0x1FA	Invalid arguments, prefetchPeriodMilliSec is set while prefetch is disabled
NSERR_CACONF_CNFL_PREFETCHMILI_PREFETCHSEC	507	0x1FB	Conflicting arguments, prefetchPeriodMilliSec and prefetchPeriod
NSERR_CACONF_ARG_LE_MIN_VAL	508	0x1FC	Invalid arguments, given value is less than the minimum value
NSERR_CACONF_ARG_GE_MAX_VAL	509	0x1FD	Invalid arguments, given value is more than the maximum value
NSERR_CACHEGROUP_NEGMINHIT	510	0x1FE	ContentGroup cannot have negative minHit.
NSERR_CACHEHA_OBJPERSIST_NOTSET	511	0x1FF	Cache Object Sync to Secondary is not set, use set cache parameter to enable.
NSERR_CACHEGROUP_INVALID_OPERATION	758	0x2f6	This operation is not permitted on selector based contentgroup

CENTRALMGMTSERVER ERRORS

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_CENTRALMGMTSERVER_REGFAILED	2047	0x7ff	Registration of device failed
NSERR_CENTRALMGMTSERVER_REQARGMISSING	2988	0xbac	Required argument missing

CFE ERRORS

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_NOSUCHIOCTL	1184	0x4a0	Command not implemented on server
NSERR_NOTARGETS	1185	0x4a1	No configured targets
NSERR_CANTRECOVER	1186	0x4a2	Configuration possibly inconsistent. Please check with the \"show configstatus\" command or reboot.
NSERR_IGNOREDIOCTL	1187	0x4a3	The command was ignored.
NSERR_REMOTECLOSE	1188	0x4a4	The remote side closed the connection.
NSERR_INVALID_TARGET	1189	0x4a5	The specified target does not exist

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_FILE_ERROR	1190	0x4a6	File operation failed
NSERR_COMMENT_DROPPED	1191	0x4a7	Failed to retain all comments
NSERR_AGGREQ_TIMEOUT	1192	0x4a8	Request to Aggregator timed out
NSERR_AGGREAD	1193	0x4a9	Failed to read data from Aggregator
NSERR_RPC_CMD_DUP	1194	0x4aa	Found unexpected RPC duplicate command
NSERR_RPC_CMD_NONDUP	1195	0x4ab	Found unexpected RPC command
NSERR_CFE_PE_COMM	1196	0x4ac	Communication error with the packet engine
NSERR_AGG_CONFAIL	1197	0x4ad	Failed to connect to the aggregator
NSERR_CFE_PE_TIMOUT	1198	0x4ae	No response from the packet engine
NSERR_AGG_INVALIDRESPONSE	1199	0x4af	Invalid response from the aggregator
NSERR_NONTPSVR	1200	0x4b0	Cannot enable ntpd when there is no ntp server configured
NSERR_AGG_SENDFAIL	1201	0x4b1	Failed to send to aggregator
NSERR_CFE_ASLEARN_COMM	1202	0x4b2	Communication error with aslearn

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_READONLY_SESSION	1203	0x4b3	Session is read-only; connect to the Cluster IP address to modify the configuration
NSERR_WRONG_PE_STATE	1204	0x4b4	The packet engine is in the wrong state to receive this command
NSERR_CFE_VALIDATION_FAILED	1205	0x4b5	Config validation failed
NSERR_XPATH_INTERNAL	1206	0x4b6	XPATH Internal Error
NSERR_CFE_CALLHOME_COMM	1207	0x4b7	Communication error with callhome
NSERR_BIND_NOENT	1208	0x4b8	No such bind resource
NSERR_PPNETMASK	1209	0x4b9	Netmask length 31 supports only point to point communications
NSERR_CFE_CLFSYNCD_COMM	1210	0X4ba	Communication error with cluster filesync server
NSERR_DB_INTERNAL	1211	0x4bb	Config DB Internal Error
NSERR_MIPDEPRECATED	1212	0x4bc	MIP is deprecated. Please use SNIP

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_VAL_INCONSITENT	1214	0x4be	Validation inconsistent between PE and configd.
NSERR_CALLHOME_LOW_HB_CUSTOM_INTERVAL	1215	0x4bf	Setting a low heartbeat interval will result in frequent CallHome uploads
NSERR_INVALIDTIMEOUT	1219	0x4c3	Invalid Timeout, it cannot be beyond admin configured value and should be between in the range of 300-86400

CLI ERRORS

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_TCPCONNFAIL	1024	0x400	Connection failed
NSERR_LOGINFAIL	1025	0x401	Login failed
NSERR_NOLOGIN	1026	0x402	Not logged in
NSERR_AUTHTIMEOUT	1027	0x403	Not logged in or connection timed out
NSERR_NOT_PRIMARY	1028	0x404	You are connected to a secondary node; configuration changes made in this session will not be propagated to, or saved on, other nodes

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_REMOTEOP	1029	0x405	Operation cannot be performed from remote login
NSERR_CONNLOST	1030	0x406	Connection with NetScaler lost
NSERR_RPCDATAMISMATCH	1031	0x407	Communication error (RPC data-size mismatch)
NSERR_RPCBADREPLY	1032	0x408	Communication error (bad RPC reply)
NSERR_UNABLETOPROMPT	1033	0x409	Unable to display secondary prompt
NSERR_LOGIN_CHALLENGED	1034	0X40A	Login challenged
NSERR_LOGOUT_SAVE	1035	0X40B	You are leaving without saving changes. Save changes now (Y/N)? [N]:
NSERR_CLEAR_CONFIG	1036	0X40C	Are you sure you want to clear the configuration(Y/N)? [N]:
NSERR_REBOOT	1037	0X40D	Are you sure you want to restart NetScaler (Y/N)? [N]:
NSERR_SHUTDOWNNS	1038	0X40E	Are you sure you want to completely stop NetScaler (Y/N)? [N]:

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_REBOOT_SAVE	1039	0X40F	Configuration not Saved. Are you sure you want to restart NetScaler (Y/N)? [N]:
NSERR_USERABORT	1040	0x410	User requested abort
NSERR_EOF	1041	0x411	EOF
NSERR_INTERRUPT	1042	0x412	Interrupted
NSERR_INTERNAL	1043	0x413	Internal error
NSERR_NOT_CLIP	1044	0x414	You are connected to NSIP of a cluster node; configuration changes made in this session will not be propagated to, or saved on, other cluster nodes
NSERR_EULA_NOT ACCEPTED	1045	0x415	End User License Agreement not accepted. Login from CLI/GUI to accept it.
NSERR_FORCE_PWDCHANGE	1046	0x416	ForcePasswordChange is enabled. Please login from CLI/GUI to change the default nsroot password
NSERR_PWD_EXISTS	1047	0x417	Default nsroot password is not allowed. Please

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
			enter a new password.
NSERR_STRMAXLEN_255	1048	0x418	String length exceeds maximum. Allowed maximum length is 255 bytes.
NSERR_STRMAXLEN_32	1049	0x419	String length exceeds maximum. Allowed maximum length is 32.
NSERR_NOPREFIX_LENGTH	1050	0x41A	Prefix length must be given with network
NSERR_INVALIDPOLLVAL	1051	0x41B	Minpoll value should not be greater than maxpoll
NSERR_SHELL_ACCESS	1052	0x41C	User has shell access
NSERR_NORESPONSE	1056	0x420	No response from NetScaler
NSERR_IOERROR	1057	0x421	I/O error
NSERR_ENV	1058	0x422	Environment error
NSERR_CMDSFAILED	1059	0x423	Some commands failed
NSERR_ALLCMDSFAILED	1060	0x424	All commands failed
NSERR_INTMINVAL_CLT_IDLETIMEOUT	1061	0x425	Integer value below minimum for client idle timeout.

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_INTMINVAL_SRV_IDLETIMEOUT	1062	0x426	Integer value below minimum for server idle timeout.
NSERR_INVALID_TCP_OPTION_TYPE	1063	0x427	Invalid tcp option type value. Allowed type values are 0 to 254
NSERR_NSINTERNAL_DEFPSWD_WARN	1064	0x428	One or more RPC nodes are configured with default passwords. For enhanced security, you must change the default RPC node password.
NSERR_OPNOTALLOW_ONCLIP	1065	0x429	Operation not permitted on CLIP
NSERR_LICEXPIRED	1066	0x42A	Features(s) license expired
NSERR_FEATDISABLED	1067	0x42B	Feature(s) not enabled
NSERR_LESS_PE	1068	0x42C	Operation not permitted. PE pool is not enough to enable additional management CPU
NSERR_MAXLIMIT	1072	0x430	Maximum resource limit reached
NSERR_SET_NOSUPPORT	1073	0x431	Set operation not supported

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_INVALIDVALUE	1074	0x432	Invalid value
NSERR_INVALIDNAME	1075	0x433	Invalid name; names must begin with an alphanumeric character or underscore and must contain only alphanumerics, '_', '#', '.', ' ', ':', '@', '=' or '-'
NSERR_INVALIDPASSWORD	1076	0x434	Invalid password. Password must contain atleast one lower case character, one upper case character, one numeric character and one special character when strong password is enabled.
NSERR_INVALIDMINPASSWORDLENGTH	1077	0x435	Minimum password length should be greater than or equal to 8 when strong password is enabled
NSERR_ENABLINGPASSWORDCOMPLEXITY	1078	0x436	Strong Password now enabled. Please ensure all the existing user passwords adhere to this restriction. Minimum Password Length is set to 8 as default.

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_INVALIDPASSWORDLENGTH	1079	0x437	Password length should adhere to minimum password length value in system parameter settings.
NSERR_CANNOTSETMINPASSWORDLENGTH	1080	0x438	Strong Password needs to be enabled to set the Minimum Password Length value.
NSERR_NOSUCHCMD	1088	0x440	No such command
NSERR_CMDAMBIGUOUS	1089	0x441	Ambiguous command name
NSERR_NOSUCHARG	1090	0x442	No such argument
NSERR_ARGVALMISSING	1091	0x443	Required argument value missing
NSERR_ARGSMUTEX	1092	0x444	Arguments cannot both be specified
NSERR_ARGPREREQ	1093	0x445	Argument pre-requisite missing
NSERR_ARGSTOOFEW	1094	0x446	Too few arguments
NSERR_ARGMISSING	1095	0x447	Required argument missing
NSERR_ARGORDER	1096	0x448	Argument(s) out of order

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_ARGVALBAD	1097	0x449	Invalid argument value
NSERR_ARGVALSEQ	1098	0x44A	Arguments cannot have the same value
NSERR_ARGAMBIGUOUS	1099	0x44B	Ambiguous argument name
NSERR_SYNCGSLBCONFIG	1100	0x44C	Please confirm whether you want to sync-config (Y/N)? [N]:
NSERR_SYNCGSLBCONFIG_WARN	1101	0x44D	Configuration mismatch with the slave sites will result in the master site's configuration prevailing on the slave sites. This might result in disruptions in traffic.
NSERR_FORCESYNCGSLBCONFIG_WARN	1134	0x46e	GSLB configuration will be removed from the slave sites and the master site's configuration will be applied to the slave sites. Traffic disruptions might occur during forced synchronization.
NSERR_ARGVALSNEQ	1104	0x450	Arguments must have the same value
NSERR_ARGVALAMBIGUOUS	1105	0x451	Ambiguous argument value

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_STRMAXLEN	1106	0x452	String length exceeds maximum
NSERR_STRMINLEN	1107	0x453	String too short
NSERR_INTMAXVAL	1108	0x454	Integer value exceeds maximum
NSERR_INTMINVAL	1109	0x455	Integer value below minimum
NSERR_INVALIDIP	1110	0x456	Invalid IP address
NSERR_INVALIDNETMASK	1111	0x457	Invalid netmask
NSERR_TOOMANYVALS	1112	0x458	Argument has too many values
NSERR_BADRANGE	1113	0x459	Range minimum exceeds range maximum
NSERR_EXPRQUOTES	1114	0x45A	Expression must be enclosed in quotes
NSERR_BADQUOTES	1115	0x45B	Unmatched quote
NSERR_INVALIDRANGE	1116	0x45C	Invalid range specification
NSERR_MISMATCHRANGES	1117	0x45D	Ranges are different sizes
NSERR_MULTIRANGES	1118	0x45E	Only one range allowed per argument

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_NOMATCHCHAR	1119	0x45F	Unmatched character
NSERR_NEEDREBOOT	1120	0x460	The configuration must be saved and the system rebooted for these settings to take effect
NSQ_SAVECONFIG	1121	0x461	Do you want to save the new configuration?
NSERR_NOTSAVED	1122	0x462	The configuration changes were not saved - they will be lost on the next reboot
NSERR_CMDEXEC	1123	0x463	Error(s) occurred - some or all changes may not be applied
NSQ_REBOOT	1124	0x464	Do you want to reboot the system now?
NSERR_NOREBOOT	1125	0x465	The configuration changes will not take effect until the system is rebooted
NSERR_PGMFAILED	1126	0x466	External program failed
NSERR_CTXMODE	1127	0x467	Contextual CLI mode
NSERR_CMDINCOMPLETE	1128	0x468	Incomplete command

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_CMDOUTOFCTX	1129	0x469	Command not valid here
NSERR_CONFIGSAVED	1130	0x46A	The running configuration has been saved
NSERR_CONFIGCLEARED	1131	0x46B	The running configuration has been cleared
NSERR_REBOOTING	1132	0x46C	NetScaler is rebooting now
NSERR_NOCONFIGSAVE	1133	0x46D	The running configuration has not changed
NSERR_REGEXNOANCHOR	1135	0x46F	First character of regular expression must be '\^'
NSERR_REGEXNOMATCH	1136	0x470	Regular expression does not match
NSERR_REGEXINVALID	1137	0x471	Invalid regular expression
NSERR_REGEXNOTALLOWED	1138	0x472	Regular expression not allowed
NSERR_REGEXNOCMD	1139	0x473	No matches
NSERR_INVALIDIPV6_FORMAT	1140	0x474	Invalid IPv6 address
NSERR_INVALIDIPV6_TWO_DOUBECOLON	1141	0x475	Double-colon can appear only once in an IPv6 address

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_INVALIDIPV6_NOPREFIX_LENGTH	1142	0x476	Prefix length must be given with an IPv6 address
NSERR_INVALIDIPV6_PREFIX_VALUE	1143	0x477	Prefix length must be in the range of 0-128
NSERR_TERMNAMEINVALID	1144	0x478	Invalid term name
NSERR_TERMINVALID	1145	0x479	Invalid syntax in term
NSERR_FORCEFAILOVER	1146	0x47a	Please confirm whether you want force-failover (Y/N)? [N]:
NSERR_FORCEFAIL_HEALTH_WARN	1147	0x47b	Force Failover may cause configuration loss, peer health not optimum. Reason(s):
NSERR_HELLOTIME_MULTIPLE	1148	0x47c	Invalid value. Hellotime Interval must be a multiple of 200
NSERR_FORCESYNCSAVE	1149	0x47d	Do you want to save the config after sync (Y/N)? [Y]:
NSERR_ERROUTFILENAME	1150	0x47e	Character '/' not allowed in outfilename
NSERR_RNATIPDEL	1151	0x47f	address is bound to rnat config, can not be removed

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_INVALIDALIAS	1152	0x480	Invalid alias
NSERR_NOSUCHALIAS	1153	0x481	No such alias
NSERR_ALIASEXISTS	1154	0x482	Alias already exists
NSERR_NOSUCHFILE	1155	0x483	No such file
NSERR_NOTREGFILE	1156	0x484	Not a file
NSERR_DEPRCMD	1157	0x485	Command deprecated
NSERR_DEPRARG	1158	0x486	Argument deprecated
NSERR_NOTLOGFILE	1159	0x487	Not a NetScaler log file
NSERR_NOPLENFORIPV6RANGE	1160	0x488	Prefix length cannot be specified for an IPv6 range
NSERR_INVALIDINT	1161	0x489	Integer not in range
NSERR_CMDAMBIGUOUS_USECOMPLETIONSOPTIONS	1162	0x48A	Ambiguous (use cmd completion for options)
NSERR_METADATA_INVAL_ENTITYTYPE	1163	0x48B	Invalid Entity Type
NSERR_SETNOTEXIST	1164	0x48C	set operation does not exist

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_SETARGNOTEXIST	1165	0x48d	set operation for one of the modified argument does not exist
NSERR_INVALID_DS	1166	0x48e	Invalid datasource
NSERR_NOSUCHCOUNTER	1167	0x48F	No such counter
NSERR_INVALIDIPMASK	1168	0x490	Invalid IP address mask
NSERR_INVALIDIPPAT	1169	0x491	Invalid IP address pattern
NSERR_BADRC	1170	0x492	Unexpected return code
NSERR_INVALIDRANGETYPE	1171	0x493	Inappropriate range values for value type
NSERR_INVALIDRANGEVAL	1172	0x494	Invalid range value
NSERR_INVALIDIPV6_PREFIX_LENGTH	1173	0x495	Prefix length must not be given
NSERR_ENTITYDELETE_FAIL	1174	0x496	Can not delete active entity
NSERR_DONE	1175	0X497	This is the last result
NSERR_RNATIPDEL2	1176	0x498	An RNAT address requires an IP address to exist

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_INCOMPATIBLEIP	1181	0x49d	Private IP and public IP must be either IPv4 or IPv6
NSERR_TRANSCR_IP	1182	0x49e	For transparent CR vserver, you cannot specify IP address
NSERR_PASSWORD_MISMATCH	1183	0x49f	Passwords entered do not match
NSERR_LEADING_TRAILING_SPACES	1053	0x41d	Leading or Trailing spaces in string
NSERR_SAVENOTDONE	1054	0x41e	The running configuration is not saved
NSERR_NOT_USED	1055	0x41f	Use this.
NSERR_INVALIDIP_VSVRTYPE	1178	0x49a	Invalid IP address or Vserver Type
NSERR_HELLOTIME_DEADINTERVAL_COMBINATION	1177	0x499	The Hello Interval must be set to 200 msec when dead interval is less than 3 sec
NSERR_MAXSESSION	1179	0x49b	Maxsession cannot be set for this user
NSERR_NEEDREPLICATE	1180	0x49c	This command will not be propagated to the other cluster nodes as you are connected to the NSIP of this cluster node

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_HDOSP_DEPRECATED	3917	0xF4D	HTTP DOS protection feature is no longer supported. Please use AppQOE feature.
NSERR_PQ_DEPRECATED	3871	0xF1F	Priority Queuing feature is no longer supported. Please use AppQOE feature.
NSERR_IOH_DEPRECATED	3870	0xF1E	Sure Connect feature is no longer supported. Please use AppQOE feature.
NSERR_NOT_PRIVATE_EXPORT	1069	0x42D	Private entities can not be exported
NSERR_OBJECT_IN_USE	1070	0x42E	Object in use, cannot delete
NSERR_CERBUNDLE_NOT_FOUND	1071	0x42F	Certbundle name not found in mapping file
NSERR_GSLB_RENAME_ONCE	1082	0x43A	Conducting multiple renaming operations on the same site in close succession may lead to synchronization inconsistencies.
NSERR_CERTBUNDLE_CANNOT_OPEN_PID	1086	0x43E	Cannot open nscertforgerd pid file

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_FAILED_TO_APPLY	1087	0x43F	Failed to apply new cert bundle
NSERR_AWS_UNSUP	1103	0x44F	Command not supported on AWS VPX
NSERR_POOLED_VPX	1102	0x44E	Ensure to provision the VPX with the recommended settings for this Bandwidth.
NSERR_GCP_UNSUPPORTED_MTU	2439	0x987	MTU greater than 1460 bytes is not supported on this platform.
NSERR_AWS_UNSUPPORTED_MTU	2440	0x988	MTU greater than 9000 bytes is not supported on this platform.
NSERR_INVALID_QUERYTYPE_FOR_IPV6	2441	0x989	Cannot use ipv6Address option with querytype set to A
NSERR_INVALID_CLIENTIP_TCPOPTION	2438	0x986	Invalid tcp option number for client ip
NSERR_ESX_UNSUPPORTED_MTU	1518	0x5ee	MTU greater than 9000 bytes is not supported on this platform.
NSERR_DYNAMIC_MESSAGE	407	0x197	

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_PASSWORDREUSE_MESSAGE	1081	0x439	

CLOUDPARAM ERRORS

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_UUID_FORMAT	3563	0xdeb	Invalid UUID format
NSERR_CUSTID_FORMAT	3564	0xdec	Invalid Citrix Cloud Customer ID format
NSERR_FQDN_FORMAT	3565	0xded	Invalid FQDN format

CLUSTER ERRORS

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_CLNOTEXIST	2448	0x990	Cluster does not exist
NSERR_TOOMANYCLS	2449	0x991	This node is already added to another cluster
NSERR_RMLOCALNODE	2450	0x992	Local Node cannot be deleted
NSERR_BKPLANEENABLED	2451	0x993	Cluster Backplane is enabled on this interface

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_LOCALNODE_NOTCONFIGURED	2452	0x994	Clustering cannot be enabled as the local node is not a member of the cluster.
NSERR_HACL_CANNOT_COEXIST	2453	0x995	Clustering and HA cannot coexist.
NSERR_CLACPKEYNOTCRT	2454	0x996	LACP key for Node/ cluster is not correct
NSERR_CLNODE_EXIST	2455	0x997	already in cluster
NSERR_BKPLANEDISABLED	2456	0x998	Disabling Cluster backplane interface
NSERR_CLAGTHROUGHPUT	2457	0x999	Currently throughput settings are not allowed on CLAG
NSERR_LICMISMATCH	2458	0x99A	License mismatch between Configuration Coordinator and local node
NSERR_CLIP_INVALIDNETMASK	2459	0x99B	CLIP netmask should be 255.255.255.255
NSERR_BKPLANELACPDELETE	2460	0x99C	This is the last interface in LACP channel configured as backplane
NSERR_LINKSETMEMBER	2461	0x99D	Interface/Channel is Linkset member.

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_CONFIG_PARAM	2462	0x99E	Setting up of NetScaler parameter ignored using this command in HA/ Cluster mode. Use 'set nsparam' command for this purpose.
NSERR_CLIP_INVALIDPREFIXLEN	2463	0x99F	CLIP prefix length should be 128.
NSERR_CLUSTER_L2NOTSUPP	2464	0x9A0	L2 Mode not supported in Cluster mode.
NSERR_LINKSET_ONEPERNODE	2465	0x9A1	Linkset can have only one Interface/ Channel per Node
NSERR_LINKSET_NOTBOUND	2466	0x9A2	Interface/Channel not bound to Linkset
NSERR_LINKSET_IDINVALID	2467	0x9A3	Linkset name should be of form LS/, id range:1-32
NSERR_CLUSTER_NBNOTSUPP	2468	0x9A4	CloudBridge is not supported in Cluster mode.
NSERR_CLUSTER_VPNNOTSUPP	2469	0x9A5	SSLVPN is not supported in Cluster mode.
NSERR_CLUSTER_AAANOTSUPP	2470	0x9A6	AAA is not supported in Cluster mode.

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_CLUSTER_IPSECNOTSUPP	2471	0x9A7	IPSEC is not supported in Cluster mode.
NSERR_LINKSET_LAMEMBER	2472	0x9A8	Interface part of a Channel
NSERR_CLIP_LOCALNODE_NOTCONFIGURED	2473	0x9A9	CLIP cannot be added as the local node is not a member of the cluster.
NSERR_CLVERSIONMISMATCH	2474	0x9AA	Cluster version mismatch between Configuration Coordinator and local node
NSERR_CLUSTER_CMNOTSUPP	2475	0x9AB	Connection Mirroring is not supported in Cluster mode
NSERR_ARP_CLAG_OWNERNODE_MANDATORY	2476	0x9AC	Owner Node should be specified for CLAG.
NSERR_ARP_OWNERNODE_MANDATORY	2477	0x9AD	Owner Node should be specified.
NSERR_NOOPCCO	2478	0x9AE	Operation not permitted on the Configuration Coordinator.
NSERR_SPOTTED_CONFIG_PRESENT	2479	0x9AF	Operation not permitted as the node is part of

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
			spotted entity configuration.
NSERR_NOT_CLUSTER_IP	2480	0x9B0	IP address should be a CLIP address.
NSERR_CLUSTER_NNRES	2481	0x9B1	Error in communication with other nodes in the cluster
NSERR_LAST_CLUSTER_IP_REMOVAL	2482	0x9B2	A NetScaler cluster must have a minimum of one cluster IP address. This is the last available cluster IP address and hence it cannot be deleted.
NSERR_CONFIG_PARAM_INVALID	2483	0x9B3	Configured Param(s) too small for Cluster. Parameter value(s) will be bumped to OVS node count.
NSERR_CLUSTER_INVALIDNODE	2484	0x9B4	Owner node value should be between 0 and 31, both inclusive.
NSERR_LRONCLACPONLY	2485	0x9B5	Link Redundancy can be set only in Cluster LACP Channels
NSERR_MULTIBIND_NOT_SUPPINCLUSTER	2486	0x9B6	Multiple Bindings in Single Bind Command not Supported in Cluster.

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_CLUSTER_FISNAMES_DUPNOTALLOWED	2487	0x9B7	In a cluster setup, the FIS name on each node must be unique.
NSERR_CLUSTER_CLAG_NOLOCALINTF	2488	0x9B8	CLA cannot be bound to the FIS as the CLA does not contain a local interface.
NSERR_FIS_MAX_LIMIT	2489	0x9B9	An appliance can have a maximum of 64 failover interface sets (FIS). This appliance or ownernode (cluster) already has maximum number of allowable FIS.
NSERR_BOUND_TO_FIS	2490	0x9BA	Interface bound to FIS.
NSERR_CHANNEL_OPEN_FAILED	2491	0x9BB	Unable to open channel
NSERR_NOT_BOUND_TO_FIS	2492	0x9BC	Interface not bound to this FIS
NSERR_CLUSTER_INC_NOTSUPP	2493	0x9BD	Feature not supported when cluster is configured in INC mode
NSERR_CONFIG_NG_CHANGED	4095	0xfff	Config NodeGroup changed, force cluster sync should be fired on newly

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
			added node to be in sync
NSERR_STRIPED_IP_EXIST	2494	0x9BE	Striped SNIPs/MIPs must be removed when transitioning to cluster-inc
NSERR_WRONG_NG	2495	0x9BF	All cluster nodes should be bound to DEFAULT_NG before transitioning to cluster-inc
NSERR_NG_REQUIRED	2496	0x9C0	The nodegroup parameter is mandatory when the -inc parameter is enabled
NSERR_NG_CHANGE	2497	0x9C1	NodeGroup can be changed only for transition from cluster to cluster-inc
NSERR_NG_INVALID	2498	0x9C2	Invalid nodegroup
NSERR_NOT_LAST_NODE	2499	0x9C3	The -flushall parameter can be enabled only when there is one node in the nodegroup
NSERR_MULTI_NG_BINDING_EXIST	2500	0x9C4	More than one Nodegroup has nodes bound to it
NSERR_INVALID_NC_CONFIG	2501	0x9C5	The owner group parameter is applicable only when

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
			the INC parameter is enabled on the cluster instance
NSERR_LS_CLAG_INTF_SAME_NG	2503	0x9C7	All interfaces of LinkSet/CLAG should belong to same nodegroup
NSERR_NODE_BINDING_INC	2504	0x9C8	Node cannot be bound to Default nodeGroup on cluster-inc setup
NSERR_IP_OWNERDOWN_PARAM	2522	0x9DA	OwnerDownResponse allowed only for spotted SNIP on cluster
NSERR_INVALID_LS	2411	0x96b	Invalid linkset
NSERR_IP_ALREADY_OWNED	2541	0x9ed	Cannot add ip address as the address is already owned by cluster or peer node
NSERR_LS_UNABLE_GET_VLAN	2542	0x9ee	Unable to get the current vlan of this linkset.
NSERR_LS_NOT_BOUND_VLAN	2543	0x9ef	Linkset not a member of this vlan
NSERR_CL_UNSUPPORTED_PROTO	2544	0x9f0	Retain connections on joining a new node is not supported for this protocol

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_CL_UNSUPPORTED_IN_NCORE	2545	0x9f1	This feature/option is not supported in n-core
NSERR_NO_SETTING_PROP	2546	0x9f2	This setting will not be propagated to other nodes.
NSERR_OWNERNODE_ALLOWED_ON_CLU	2547	0x9f3	ownerNode setting is allowed only on CLIP.
NSERR_CL_NOT_DFLT_NG	2548	0x9f4	In L2 cluster, adding a node with nodegroup other than DEFAULT_NG is not permitted.
NSERR_CL_RECOVERY_IN_PROGRESS	2555	0x9fb	Operation not permitted - Cluster node recovery is in progress.

CQA ERRORS

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_CQA_LABEL_3_NOTSET	3782	0xec6	Network type net3 is not set
NSERR_CQA_WRONG_COEF	3783	0xec7	Coefficient values are not proper Need to give intercept and one feature from list. Check man page
NSERR_CQA_WRONG_CCL	3784	0xec8	Congestion level scale is not proper

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_CQA_WRONG_CSQ	3785	0xec9	Signal Quality scale is not proper
NSERR_CQA_LR1_DEPENDENCY	3786	0xeca	Need to set network type net1 and net2
NSERR_CQA_LR2_DEPENDENCY	3787	0xecb	Need to set network type net2 and net3
NSERR_CQA_WRONG_LOG_COEF	3788	0xecc	Log Coefficient values are not proper
NSERR_CQA_LABEL_1_NOTSET	3789	0xecd	Network type net1 is not set
NSERR_CQA_LABEL_2_NOTSET	3791	0xecf	Network type net2 is not set

CR ERRORS

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_PXY_CACHE_HMG	512	0x200	All caches in a content group should be of the same type
NSERR_PXY_RM_LAST_MEMT	513	0x201	Cannot remove last map entry from the table; remove the map table instead
NSERR_CSW_INS_INVAL_PFX	514	0x202	Invalid prefix specified in the URL
NSERR_PENG_EXPR_IVAL_NAME	515	0x203	Invalid expression name

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_CSW_BIG_URL	516	0x204	URL specified is too long - maximum is 208, including . and *
NSERR_CSW_BIG_PFX	517	0x205	Prefix specified is too long - maximum is 199, excluding *
NSERR_CSW_BIG_SFX	518	0x206	Extension specified is too long, maximum is 8
NSERR_CSW_INVAL_SFX	519	0x207	Extension is invalid
NSERR_EXPR_NOMETHOD	520	0x208	Invalid method name
NSERR_EXPR_NOURLTOKENS	521	0x209	Invalid HTTP URL tokens
NSERR_EXPR_NOVERSION	522	0x20A	Invalid HTTP version
NSERR_EXPR_NOHDR	523	0x20B	Invalid HTTP header
NSERR_EXPR_NOCACNTL	524	0x20C	Invalid cache-control value
NSERR_EXPR_NOPRAG	525	0x20D	Invalid pragma value
NSERR_EXPR_NOQUERY	526	0x20E	Invalid query string
NSERR_EXPR_NOQUAL	527	0x20F	Invalid qualifier
NSERR_ACTION_INUSE	528	0x210	Action name is already in use

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_ACTION_HDR_INVAL	529	0x211	Invalid header
NSERR_URLQ_INVAL	530	0x212	
NSERR_UNDEF_ACTION	531	0x213	Action directive or qualifier is not valid
NSERR_CPE_INUSE	532	0x214	Policy name is already in use
NSERR_CPE_REQACT_INVAL	533	0x215	Request action is not valid
NSERR_CPE_RSPACT_INVAL	534	0x216	Response action is not valid
NSERR_CPE_REQRULE_INVAL	535	0x217	Request rule is not valid
NSERR_ACTION_DEFINVAL	537	0x219	Default actions cannot be removed
NSERR_ACTION_NOTPRESENT	538	0x21A	Action does not exist
NSERR_PXY_INVAL_SERVICETYPE	539	0x21B	Invalid service type for virtual server
NSERR_CACHEPOLICY_INUSE	540	0x21C	Caching policy name is already in use
NSERR_CACHEGROUP_INTERNAL	543	0x21F	Built-in content groups cannot be removed
NSERR_CPE_INVAL	544	0x220	Policy name is invalid

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_EXPR_NOLEN	545	0x221	URL length is not valid
NSERR_DNSWAIT	546	0x222	
NSERR_GW_TIMEOUT	547	0x223	
NSERR_CSWDMN_INUSE	548	0x224	Domain is already hosted by another server
NSERR_CSWDMN_PLCY_EXIST	549	0x225	
NSERR_ACTION_NOMOD_HDR	550	0x226	Action has missing argument
NSERR_EXPR_INVAL_OPERATOR	551	0x227	Invalid operator for the qualifier
NSERR_EXPR_DEF_REM_INVAL	552	0x228	Default expression cannot be removed
NSERR_EXPR_TOOMANY	553	0x229	Expression limit reached
NSERR_ACTION_TOOMANY	554	0x22A	Action limit reached
NSERR_CSWPOLICY_TOOMANY	555	0x22B	CS policy limit reached
NSERR_CRDPOLICY_TOOMANY	556	0x22C	CR policy limit reached
NSERR_MAPPOLICY_TOOMANY	557	0x22D	Map policy limit reached
NSERR_FILTER_NOT_SUPPORT	558	0x22E	Content Filtering is no longer supported;

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
			this feature flag will be removed on the next major release
NSERR_CACHEPOLICY_TOOMANY	559	0x22F	Integrated cache policy limit reached
NSERR_CACHEGROUP_TOOMANY	560	0x230	Integrated cache content group limit reached
NSERR_CACHEPARAM_MEMALLOC_FAILED	561	0x231	Unable to allocate specified amount of memory
NSERR_CACHEGROUP_INUSE	562	0x232	Content group name is already in use
NSERR_CACHEGROUP_EXPCONFLICT	563	0x233	Expiry times conflict
NSERR_CACHEPARAM_INVAL	564	0x234	Cache parameter is invalid
NSERR_CACHEGROUP_PARAM_INVAL	565	0x235	Invalid invalidation parameter
NSERR_CACHEGROUP_QUERY_INVAL	566	0x236	Invalid query string
NSERR_ACTION_INVAL	567	0x237	Action name is invalid
NSERR_EXPR_DEF_SET_INVAL	568	0x238	Default expression cannot be set

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_CACHEGROUP_RESSZ_MIN_GT_MAX	569	0x239	Minimum response size cannot exceed the maximum response size
NSERR_SVPN_CERT_CHALLENGE	571	0x23B	Destination Server challenged for a client certificate
NSERR_CACHEGROUP_HOST_REQ	576	0x240	Host required for a group with invalidation restricted to host
NSERR_CACHEGROUP_HOST_NREQ	577	0x241	Host not required
NSERR_CACHEGROUP_DYNGRP_NEXP	578	0x242	Cannot expire a parameterized content group
NSERR_CACHEGROUP_ONE_GRP_REQ	579	0x243	Only one content group required
NSERR_CACHEGROUP_ONE_ALL_REQ	580	0x244	ALL should be the only content group specified
NSERR_CACHEGROUP_MATCH_PARAM_INVAL	581	0x245	Invalid request hit parameter
NSERR_CACHEGROUP_DYN_RES_CACHE	582	0x246	Cannot specify a parameterized group with a response time CACHE action
NSERR_EXPR_INVAL_VALUE	583	0x247	Invalid expression value

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_CACHEGROUP_PREFETCH_CONFLICT	584	0x248	Prefetch periods conflict
NSERR_CACHEGROUP_PREFETCH_ENABLE	585	0x249	Enable prefetch to set prefetch period
NSERR_CACHEGROUP_CCH_UNKNOWN	586	0x24A	Unknown cache-control header
NSERR_CACHEGROUP_RELEXP_X10MS	587	0x24B	Relative expiry milliseconds must be multiples of 10
NSERR_CACHEGROUP_PREFETCH_X10MS	588	0x24C	Prefetch period milliseconds must be multiples of 10
NSERR_CACHEGROUP_STATIC_TO_DYNAMIC	589	0x24D	This content group cannot be made parameterized
NSERR_CLASSIC_POLICY_DEPRECATED	590	0x24E	Classic policy expressions are deprecated, are not supported, and will be removed in the next major release - use Default (Advanced) policy expressions instead; the nspepi utility may be helpful in conversion
NSERR_PLCY_DEF_REM_INVAL	591	0x24F	Default policy cannot be removed

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_CACHEGROUP_PREFETCH_REL_NREQ	592	0x250	Relative expiry and prefetch period should both be seconds or milliseconds
NSERR_EXPR_SET_INVAL_FLOWTYPE	593	0x251	Flow type cannot be changed
NSERR_EXPR_TOO_BIG	594	0x252	Expression too long - maximum length is 1500, in fully-qualified form
NSERR_CPE_INVALID_IDRANGE	595	0x253	Priority should be between 0 and 64000 (inclusive)
NSERR_EXPR_TOO_BIG_EXT	596	0x254	Expression too long - maximum length is 800, in fully-qualified form
NSERR_CACHEGROUP_MATCHCOOKIE_DYN_REQ	597	0x255	Match cookies argument allowed only with parameterized groups
NSERR_CACHEGROUP_MATCHCOOKIE_NREQ	598	0x256	Cannot modify match cookies
NSERR_CACHEFWPXY_PRESENT	599	0x257	Forward proxy is already present
NSERR_CACHE_PREFETCH_REEVAL_NREQ	600	0x258	Cannot configure a content group to both prefetch and evaluate every miss

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_CACHEFWPXY_TOOMANY	601	0x259	Forward proxy limit reached
NSERR_CACHE_PET_FC_NREQ	602	0x25A	Cannot enable both 'Poll Every Time' and 'Flash Cache'
NSERR_SAVECONFIG_IN_PROGRESS	603	0x25B	Configuration is being saved, please try again later
NSERR_GWSUBNET_NOT_EXIST	604	0x25C	The gateway is not directly reachable
NSERR_GW_REQ_SUBNET	605	0x25D	An existing route relies on the presence of this subnet
NSERR_BAD_CR_ATTRIBS	607	0x25F	Bad cache redirection VIP attributes given
NSERR_MAC_NOT_SUPPORTED	608	0x260	MAC redirection not supported
NSERR_POLICY_NOT_SUPPORTED	609	0x261	Policy redirection not supported with NNTP
NSERR_CACHEABILITY_NOT_SUPPORTED	610	0x262	Cannot set cacheability on cache
NSERR_HOST_RT_NOT_ALLOWED	611	0x263	Host route advertisement not permitted for this IP

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_ROUTING_NOT_ALLOWED	612	0x264	Routing protocols can run only on SNIP's or NSIP
NSERR_CONFIG_NOTSAVED	613	0x265	Configuration is not saved
NSERR_DIS_ROUTING_NSIP	614	0x266	Cannot disable dynamic routing on NSIP
NSERR_NETWORK_RT_NOT_ALLOWED	615	0x267	Network route advertisement not permitted on this IP
NSERR_NR_ENABLE	616	0x268	networkRoute can be enabled only for one IP per subnet
NSERR_EXPRMISMATCH	624	0x270	
NSERR_NO_HOST	627	0x273	No host header and default not set
NSERR_NO_DFLT	628	0x274	Host header present, no match, and default not set
NSERR_DFLTDMN_FIRST	629	0x275	No default domain translation entry
NSERR_PXY_CONF_LOOP	630	0x276	Source and target domains cannot be the same
NSERR_PXY_ME_DUP	632	0x278	Duplicate map entry

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_PXY_IVAL_TGT	633	0x279	Target is invalid during map entry addition
NSERR_CONNECTED	634	0x27A	Proxy connection established
NSERR_AUTHENTICATE	635	0x27B	Authentication required
NSERR_LARGE_DOMAIN	636	0x27C	Domain length overflow
NSERR_PXY_IVAL_URL	640	0x280	Source/destination URL or the combination is not valid
NSERR_PXY_ME_USE	641	0x281	Map entry is already in use
NSERR_PXY_MT_TYPE	642	0x282	Map entries in a table should be homogeneous
NSERR_PXY_MT_USE	643	0x283	Map table is in use
NSERR_PXY_MB_INVAL	644	0x284	Invalid map bind operation
NSERR_PXY_MB_USE	645	0x285	You can bind only one table to a vserver
NSERR_PXY_SETDCDN	646	0x286	Invalid DCDN configuration
NSERR_PXY_SETDFLT	647	0x287	Invalid default domain specification

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_PXY_DFLT_NOTSET	648	0x288	Removing default without setting it
NSERR_PXY_FWD_IVAL	649	0x289	Invalid FWD PXY map entry
NSERR_PXY_MTX_PROT	656	0x290	PXY and cache protocol should be the same
NSERR_PXY_MTX_TRA	657	0x291	Invalid cache type on service
NSERR_PXY_MTX_FWD	658	0x292	Forward Pxy matrix
NSERR_PXY_MTX_REV	659	0x293	Reverse Pxy Matrix
NSERR_PXY_ADD_TRA_NONHTTP	660	0x294	transparent non-HTTP policy is invalid
NSERR_PXY_ADD_TRA_OTHER	661	0x295	transparent non-HTTP map/via should not be specified
NSERR_PXY_OPT_INVAL	662	0x296	ARP/ghost options invalid for REV/FWD proxy
NSERR_PXY_ADD_SVR_OTHER	663	0x297	Simple content based no proxy attribs
NSERR_PXY_MB_DUP	664	0x298	Bind entry already exists

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_PXY_DFLT_DUP	665	0x299	Default already exists
NSERR_SEL_INUSE	672	0x2a0	Selector already exists
NSERR_SEL_PARSE_FAILED	673	0x2a1	Error in selector expression syntax
NSERR_NOSELECTOR	674	0x2a2	No such selector
NSERR_SEL_TOOMANY	675	0x2a3	Selector limit reached
NSERR_CACHEGROUP_NOSELPARAM	677	0x2a5	Cannot change param-based content group to selector-based (or vice-versa)
NSERR_NOCACHEGROUP	678	0x2a6	Content group does not exist
NSERR_NONREQ_SEL	679	0x2a7	Selector expression is not request based
NSERR_INVALARG	680	0x2a8	The action qualifier and the specified argument(s) do not match
NSERR_NOWILD_ALLOWED	681	0x2a9	Wildcard not allowed with BETWEEN operator
NSERR_DATE_INCOMPAT	682	0x2aa	Time arguments incompatible
NSERR_TIMEDATE_INVALID	683	0x2ab	Date/time value invalid

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_CONTENTGROUP_COOKIE_REQ_PARAM	684	0x2ac	Hit parameters or inval parameters needed to enable cookie matching
NSERR_CONTENTGROUP_IGNORECASE_REQ_HITPARAM	685	0x2ad	Hit parameters needed to enable case-insensitive param value matching
NSERR_CONTENTGROUP_INVALPARAM_REQ	686	0x2ae	Inval parameters needed to enable host-based invalidation
NSERR_CLISEC_EXP_TOO_LONG	687	0x2af	Client security expression too long
NSERR_NONHTTP_CSW_BIND_HTTP_SSL_POLICY	688	0x2b0	HTTP/SSL protocol based policies can be bound only to HTTP/SSL CS vserver
NSERR_POLBOUNDTO_TOO_MANY_VSVRS	691	0x2b3	Domain cannot be set - policy bound to more than one vserver.
NSERR_PRIORITY_COMP_PI_CSW	695	0x2b7	Priority is mandatory for advanced expressions.
NSERR_PE_GOTO	697	0x2b9	Priority Jump expression cannot be bound with a classic expression based policy.

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_CACHEOBJECT_EVICT	699	0x2bb	Cached object removed on expiry.
NSERR_DNSFAIL	700	0x2bc	DNS request failed
NSERR_HC_RET_TYPE_CHANGE	701	0x2bd	Cannot change callout return type.
NSERR_HC_NOT_HTTP_VS	702	0x2be	Not a HTTP or SSL vserver.
NSERR_HC_REQ_CONFIG_XOR	703	0x2bf	Full request expression and other request attributes cannot be set at the same time.
NSERR_HC_SERVICE_CONFIG_XOR	704	0x2c0	and vserver cannot be set at the same time.
NSERR_HC_RET_TYPE_REQD	705	0x2c1	Return type needs to be configured first.
NSERR_CSW_BIND_INCOMPAT_TGT	707	0x2c3	The target vserver is not compatible with the CS verver.
NSERR_CSW_BIND_INCOMPAT_CSPL	725	0x2d5	The target vserver is not compatible with the CS policylabel.
NSERR_AS_BAD_XMLNAMESPACE_PREFIX	708	0x2c4	Invalid XML-Namespace prefix.
NSERR_INVALID_SIP_EXPR	709	0x2c5	The SourceIP Expression specified is invalid.

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_NO_BACKENDVSERVER	710	0x2c6	No backend LB vserver found.
NSERR_CONTENT_GROUP_TOOMANY	711	0x2c7	ContentGroup limit reached
NSERR_CACHE_MEM_SIZE_CHANGED	712	0x2c8	To use new Integrated Cache memory limit, save the configuration and restart the NetScaler.
NSERR_CACHE_MEM_SIZE_ZERO	713	0x2c9	No memory limit is configured for Integrated Cache. Use set cache parameter command to set the memory limit.
NSERR_L2CONN_NOT_ALLOWED	714	0x2ca	l2conn feature is supported only for ncore.
NSERR_SQL_NOT_ALLOWED	715	0x2cb	Database feature is supported only on nCore
NSERR_IPSEC_NOT_ALLOWED	716	0x2cc	IPSec feature is not supported
NSERR_HTMLPAGE_NOT_ALLOWED	717	0x2cd	Respondwith/ sqlresponse_ok/ sqlresponse_error actions cannot be set to respondwithhtmlpage action, and vice versa.

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_CSW_NO_POLICY_NAME	719	0x2cf	Policy name is required with priority.
NSERR_SQL_MSG_EXCEED	720	0x2d0	Message length should be smaller than 512
NSERR_ROUTING_STRIPED_SNIP	722	0x2d2	Routing protocols can run only on a spotted SNIP in a cluster
NSERR_USERNAME_MISSING	723	0x2d3	UserName argument Missing
NSERR_ACTION_EXIST	724	0x2d4	Default Action for this type already exist.
NSERR_WRONG_SERVICENAME	726	0x2d6	Use corresponding 'gslb service' command.
NSERR_PE_NOT_ALLOWED_RULE	727	0x2d7	PE expressions are not allowed for RULE based persistence
NSERR_NODE_NOT_IN_CLUSTER	728	0x2d8	Node is not in the cluster
NSERR_MCMX_CNRES	729	0x2d9	Error in communication with other cores
NSERR_HC_POST_REQ_CONFIG_XOR	730	0x2da	Parameters and body cannot be set at the same time for the POST method
NSERR_HC_CACGRP	731	0X2db	Operation on 'calloutContentGroup

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
			' content group not permitted
NSERR_CSW_BIND_INCOMPAT_BKUP	732	0x2dc	The backup vserver of the target vserver is not compatible with the CS vserver.
NSERR_CACHE_MEM_RESIZE_IN_PROGRESS	733	0x2dd	Integrated Cache memory resize is in progress. Please wait a few seconds.
NSERR_CACHE_MEM_RESIZE_FAILED	734	0x2de	Integrated Cache memory resize failed.
NSERR_CSW_BIND_INCOMPAT_TARGET	735	0x2df	The target vserver has to be an LB vserver.
NSERR_ATTRIB_MEM_FREED	736	0x2e0	ATTRIB memory already freed
NSERR_RULE_MISSING	737	0x2e1	EvalRule argument Missing
NSERR_CACHEGROUP_CCH_MAXAGE_MAX	738	0x2e2	max-age value cannot be greater than 2147483647
NSERR_CACHE_MEM_REDUCTION_NOT_ALLOWED	739	0x2e3	Integrated Cache memory limit cannot be reduced.
NSERR_CSW_POL_INCOMPAT_LB	740	0x2e4	The target vserver is not compatible with the CS policy expression.

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_CS_INVALBACKUP	741	0x2e5	Content-Switching or Cache-Redirection vservers cannot be used as a backupvserver.
NSERR_CACHE_MEM_LIMIT_EXCEEDING	742	0x2e6	The IC memory configured for all the admin partitions that are defined on the appliance, must be limited to the IC memory that is configured on the default partition.
NSERR_INVAL_ARG_CRPL_LBVS	745	0x2e9	LB vserver cannot be bound to the CR vserver along with a CR policy.
NSERR_CACHE_MEM_LIMIT_NOT_CONFIGURED	747	0x2eb	Set the IC memory on the default partition before setting the IC memory for an admin partition.
NSERR_INVALID_BIND_PIPOL_CS	748	0x2ec	The Advanced Policy cannot be bound to a CS vserver
NSERR_INVALID_BIND_PIPOL_CR	749	0x2ed	The Advanced Policy cannot be bound to a CR vserver
NSERR_MEDIAC_MEMORY_ALLOC_FAILED	750	0x2ee	Memory allocation for media classification failed

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_CSPOL_VPN_BIND	756	0x2f4	Invalid bind, VPN vserver is already set as a target Vserver on a CS action.
NSERR_CSACT_VPN	757	0x2f5	VPN vserver cannot be set as a target Vserver since CS policies are bound to it.
NSERR_CSPOL_ACT_VPN	759	0x2f7	CS policy cannot be bound to the vserver. CS action must be a LB vserver.
NSERR_VPNSERVER_NOTEXIST	760	0x2f8	The VPN Vserver does not exist
NSERR_VPNREFERRED_IN_CSBINDING	761	0x2f9	Cannot remove VPN Vserver which is referred in CS policy bindings.
NSERR_DEFAULTVPN_NOT_BOUND	762	0x2fa	Default VPN mentioned is not bound
NSERR_HDXINVAL	763	0x2fb	HDX servicetype cannot have WildCard IP and Port or 0 IP.
NSERR_CSW_ACTION_INCOMPTIBLE	764	0x2fc	Incompatible Content Switching action provided. During set operation the old and the new action should have compatible fields. eg,

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
			target LB vserver to target LB vserver.
NSERR_FWPXY_LICENSE	3578	0xdfa	Feature not licensed [FORWARDPROXY]
NSERR_GSLB_SVC_GRP_VSRVR_ERR	941	0x3ad	Binding of same GSLB servicegroup to heterogeneous IPV4 and IPV6 GSLB vservers is not allowed.
NSERR_GSLB_SVC_GRP_IP_ERR	942	0x3ae	Same GSLB servicegroup cannot be bound to both IPV4 and IPV6 addresses.
NSERR_GSLB_PUB_IP_PORT	943	0x3af	This configuration change will result in inconsistent private and public ip/port combination across GSLB services/ servicegroup items.
NSERR_GSLB_SVCGRP_PUBIP_PUBPORT_EXISTS	1341	0x53d	The Public IP and Public port is being used by another service item in the same GSLB servicegroup.
NSERR_NO_GSLBSVCGRP	1349	0x545	The GSLB servicegroup does not exist

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_RENAME_GSLB_SVCGRP_WARN	1350	0x546	Please fire this command on all the participating GSLB sites manually or by using real time sync otherwise stats exchange between GSLB sites will not work.
NSERR_CS_PERSIST_NT_ALLWD	1688	0x698	Persistence is not supported for PROXY and CS GSLB type of CS vservers.
NSERR_GSLB_WC_PER_NOT_SUPPORTED	1494	0x5d6	Site persistence will not be honored for wildcard domains.
NSERR_CR_SVC_ERROR	1903	0x76f	DisallowServiceAccess option is applicable only for CR Forward Cache Type vservers.
NSERR_CACHE_MEM_MINIMUM_CRITERIA_NOT_MET	1718	0x6b6	Minimum cache memory not configured
NSERR_GSLB_DEFAULTRPCPASS_WARN	1273	0x4f9	One or more GSLB rpcNodes are configured with default password. Please change the rpcNode password for GSLB sync to work.

CVPN ERRORS

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_NO_SUCH_PROFILE	3248	0xcb0	Profile does not exist
NSERR_PROFILE_IN_USE	3249	0xcb1	Profile in use
NSERR_NO_SAML PROFILE	3383	0xd37	Please specify a SAML SSO profile.
NSERR_NO_SUCH_PUSH_SERVICE	3003	0xbbb	Push service does not exist

DSK CACHE ERRORS

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_IC_CACHE_NOT_ENB	752	0x2f0	FEO enabled but IC needs to be enabled for most FEO features to work.
NSERR_DISK_ENGG_NOT_RUNNING	753	0x2f1	Disk Engine is not running, Save the config and reboot.
NSERR_DISK_ENGG_DISABLED	754	0x2f2	To take Disk Engine down, Save the config and reboot.
NSERR_IC_DISK_CACHE_PARAM_NOT_SET	755	0x2f3	Disk Cache not enabled. Set -enableDiskCache parameter to YES.

FILEUPLOAD ERRORS

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_NO_DIR	3440	0xd70	Directory does not exist.
NSERR_NO_FILE	3441	0xd71	File does not exist.
NSERR_FILEEXT_NOTSUP	3442	0xd72	Unsupported file format. only txt/cert/req/xml/key type of files are allowed.
NSERR_FILECONT_NOTSUP	3443	0xd73	Unsupported file content. file content should be base64 encoded.
NSERR_FILEENC_NOTSUP	3444	0xd74	Unsupported encoding type. only BASE64 encoding is allowed.
NSERR_NO_DEST	3445	0xd75	Destination path does not exist.
NSERR_INVALID_DEST	3446	0xd76	User doesn't have permission for given Destination path.

FWDSESSION ERRORS

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_FWDSESSION_NAME_EXISTS	928	0x3a0	A forwarding session with same name exists

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_FWDSESSION_NW_EXISTS	929	0X3a1	A forwarding session with same network exists
NSERR_FWDSESSION_ACL_EXISTS	930	0X3a2	This acl is already configured
NSERR_FWDSESSION_ACL_NOT_EXISTS	931	0x3a3	Specified ACL is not configured
NSERR_FWDSESSION_CONN_FAILOVER	932	0x3a4	Connection fail-over not supported for v6 forwarding sessions

GENTOOL ERRORS

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_SSL_CONFFILE	1601	0x641	Error in SSL conf file
NSERR_SSL_NOCONFFILE	1602	0x642	Unable to load SSL configuration info
NSERR_SSL_SIGFAIL	1603	0x643	Signing operation failed
NSERR_SSL_INVALFORMAT	1604	0x644	Invalid format
NSERR_SSL_OUTFILE	1605	0x645	Problem in writing output file
NSERR_SSL_VERIFY_FAIL	1606	0x646	Signature verification failed
NSERR_SSL_FILECREATE	1607	0x647	Unable to create output file

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_SSL_MINKEYSIZE	1608	0x648	Key size less than 1024 is not supported on FIPS Firmware Version 1.1.
NSERR_SSL_INVALID_REQ	1609	0x649	Invalid certificate request
NSERR_SSL_GENTOOL	1610	0x64A	Internal failure in SSL cert/key generation tool
NSERR_SSL_PEM_ONLY	1611	0x64B	Only PEM format private key can be encrypted
NSERR_SSL_PASSMISMATCH	1612	0x64C	Password verification failed
NSERR_SSL_PASSREQ	1613	0x64D	Password required for private key
NSERR_SSL_INVALPASS	1614	0x64E	Invalid password
NSERR_SSL_MAXKEYSIZE	1615	0x64F	Maximum allowed key size is 2048
NSERR_SSL_GNTOOLARG_MISSING	1616	0x650	Required argument missing
NSERR_SSL_INVAL_PUBEXP	1617	0x651	Invalid public exponent value
NSERR_SSL_INVALID_VALUE	1618	0x652	Invalid value
NSERR_SSL_MISSING_KVAL	1619	0x653	Value missing for the argument

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_SSL_INVAL_DHGEN	1620	0x654	Invalid DH generator value
NSERR_SSL_NOFILE_CERTREQ	1621	0x655	No such certificate request file exists
NSERR_SSL_REQ_NOMATCH	1622	0x656	Certificate Request (CSR) and private key do not match
NSERR_SSL_PKCS12	1623	0x657	Problem in input PKCS12 file
NSERR_SSL_NOFILE_CAPVTKEY	1624	0x658	No such CA key file present
NSERR_SSL_NOFILE_CACERT	1625	0x659	No such CA certificate file exists
NSERR_SSL_NOFILE_SERIAL	1626	0x65A	No such serial file exists
NSERR_SSL_NOFILE_PKCS12	1627	0x65B	No such PKCS12 file exists
NSERR_SSL_READ_CACERT	1628	0x65C	In reading input CA certificate file
NSERR_READ_CERT	1629	0x65D	Error in reading input certificate file
NSERR_IMP_EXP_NOT_TOGETHER	1630	0x65E	Import and export can not be specified together
NSERR_NOFILE_CERT	1631	0x65F	No such certificate file exists
NSERR_NOFILE_KEY	1632	0x660	No such key file exists

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_CACERTPKEY_MISMATCH	1633	0x661	CA certificate not matching with CA private-key
NSERR_WRONG_REV_ENTRY	1634	0x662	Invalid revocation entry in CA's database
NSERR_WRONG_REV_DATE	1635	0x663	Invalid revocation data in CA's database
NSERR_WRONG_SERIAL_NO	1636	0x664	Invalid serial number in CA's database
NSERR_CREATE_DATABASE_ENTRY	1637	0x665	Revocation entry creation failed
NSERR_ALREADY_REVKD	1638	0x666	Certificate already revoked
NSERR_LOAD_PKEY	1639	0x667	Private key loading failed
NSERR_CERTPKEY_NEEDED	1640	0x668	Both certificate and private key are needed for export
NSERR_PKCS12_NEEDED	1641	0x669	PKCS12 file missing for import
NSERR_ERR_FILE EXISTS	1642	0x66A	Cannot create output file. File already exists
NSERR_FIPSKEY_KEYFILE_OPTION	1643	0x66B	Both -keyFileName and -fipsKeyName cannot be specified

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_OUTFILELENBIG	1644	0x66C	Output file name too long
NSERR_SSL_DEFPATH	1645	0x66D	Output filepath should be under the partition's default SSL directory
NSERR_SSL_CRL_DEFPATH	1646	0x66E	Output CRL filepath should be under the partition's default CRL directory
NSERR_SSL_DEFLOCATION	1647	0x66F	Input file(s) not present or not accessible in current partition
NSERR_SSL_DNS_DEFPATH	1648	0x670	Output filepath should be under the partition's default DNS directory
NSERR_SSL_CERTKEY_INCOMPATIBLE	1649	0x671	Cannot bind incompatible certkey type with Vserver.
NSERR_DHREQD	1791	0x6FF	DH required
NSERR_SSL_CRL_DEFLOCATION	1650	0x672	Input CRL file does not present or not accessible under the partition's default CRL directory
NSERR_SSL_NOFIPS_KEY	1651	0x673	No such FIPS key
NSERR_SSL_IMPROPER_SERIALFILE	1652	0x674	Invalid serial file

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_SSL_SERIAL_NUM_REVOKED	1653	0x675	Certificate serial number match with another certificate already revoked in the CRL
NSERR_SSL_MAXRSAKEYSIZE	1654	0x676	Maximum allowed key size is 4096
NSERR_SSL_MUSTBEPEM	1655	0x677	The input file must be in PEM or SIM format.
NSERR_SSL_CANTBEPEM	1656	0x678	The input file cannot be in PEM format.
NSERR_SSL_BAD_LABEL	1657	0x679	The keylabel cannot be 'public' or 'private'.
NSERR_SSL_HSMKEY_LOAD	1664	0x680	Unable to Load Key in external Hardware Security Module (HSM).
NSERR_SSL_HSMKEY_PPE	1665	0x681	Internal error while adding HSM key.
NSERR_ERR_SSL_HSMKEY_NOKEY	1666	0x682	Missing argument [Key].
NSERR_ERR_SSL_HSMKEY_DELETE	1667	0x683	Unable to Delete Key in external Hardware Security Module (HSM).
NSERR_ERR_SSL_HSMKEY_NOMATCH	1668	0x684	Specified HSM Type does not match.

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_ERR_SSL_HSMKEY_REFEXT	1669	0x685	The HSM key is referenced by a certificate
NSERR_ERR_SSL_HSMKEY_NOTEXISTS	1670	0x686	No such HSM key.
NSERR_ERR_SSL_HSMKEY_NOSTORE	1671	0x687	Specified keystore does not exist.
NSERR_ERR_SSL_GW_NOTUP	1672	0x688	Gateway daemon is booting up please wait for 20 to 30 secs.
NSERR_ERR_SSL_HSMKEY_FIPS	1673	0x689	Operation not permitted on an MPX-FIPS System.
NSERR_ERR_SSL_SANCERT_DUP	1674	0x68A	Duplicate domain cert cannot be added.
NSERR_SSL_ECDSA_SUPPORT	1675	0x68B	ECDSA certificates are not supported for this entity/platform.
NSERR_SSL_ECDSA_CURVE_SUPPORT	1676	0x68C	The EC curve in the ECDSA certificate is not supported.
NSERR_SSL_LINK_LOOP	1677	0x68D	Certificate can't be linked. This is creating a loop.
NSERR_SSL_N3FIPSREBOOT	1678	0x68E	N3FIPS InitHSM is not done, Please reboot again

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_SSL_N3FIPS_FILECREATE	1679	0x68F	FIPS config folder /nsconfig/fips is not present, please create it manually and reboot the system, after reboot reset and set fips again
NSERR_SSL_SIGHASH_SUPPORT	1680	0x690	List contains unsupported SigHash type for this entity/platform.
NSERR_SSL_SAN_CERT_ENTRY	1681	0x691	Unsupported OID for SAN entry in certificate
NSERR_CIPHER_BACKEND	1682	0x692	The cipher alias cannot be bound to this entity. It is only applicable for an SSL backend service or an SSL serviceGroup
NSERR_SSL_CIPHER_NOT_SUPPORTED_ON_PLATFORM	1683	0x693	This Cipher/CipherAlias is not supported on this platform.
NSERR_SSL_I2D_X509_NAME_FAILURE	1684	0x694	Failed to encode X509_NAME into DER format
NSERR_DTLS_CIPHER_SUPPORT	1685	0x695	This cipher alias cannot be bound. DTLS vServer/Service only supports

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
			DEFAULT_DTLS/ DEFAULT_DTLS_BACKEND ciphers respectively.
NSERR_DTLS_CIPHER_BACKEND	1686	0x696	The cipher alias cannot be bound to this entity. It is only applicable for a DTLS backend service or a DTLS serviceGroup.
NSERR_SSL_DIGEST_FIPS	1689	0x699	Digest type is not supported on this platform
NSERR_SSL_QUIC_TLS13_ONLY	1694	0x69E	SSL profiles of type QUIC Front-End only support TLS 1.3 cipher suites.
NSERR_ERR_SSL_HSMKEY_EXISTS	1695	0x69F	HSM key exists.
NSERR_ERR_SSL_HSMKEY_MEM_FAILURE	1732	0x6C4	HSM key memory allocation failed.

GRPC PB ERRORS

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_GRPC_PB_UNKNOWN_WIRE_TYPE	1704	0x6a8	Invalid Protocol Buffer wire type seen.
NSERR_GRPC_PB_KEY_NOT_FOUND	1715	0x6b3	Protocol Buffer Field not found.

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_GRPC_PB_REP_FIELD_RANGE	1716	0x6b4	Repeated Protocol Buffer field index exceeds repeated size.
NSERR_GRPC_PB_VALIDATION_FAILED	1717	0x6b5	gRPC validation failed.

GSLB ERRORS

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_BAD_DNS_OPTION	1792	0x700	Invalid DNS option specified
NSERR_DNS_BAD_CACHETYPE	1793	0x701	Only forward cache type can bind to DNS vserver
NSERR_DNS_NOTAVAIL	1794	0x702	No such DNS vserver exists
NSERR_DNS_BAD_VSTYPE	1795	0x703	DNS vserver can only be address-based
NSERR_GSLB_SITELKUP_FAILED	1796	0x704	GSLB site not found
NSERR_GSLBBOUNDTO_CSACT	1797	0x705	The GSLB Vserver referred by Content Switching action cannot be removed
NSERR_GSLBREFFERED_IN_CSBINDING	1798	0x706	Cannot remove GSLB Vserver which is referred in CS policy bindings

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_NOAREC	1801	0x709	Address record for host name not available
NSERR_INVALTTL	1806	0x70E	Invalid TTL value
NSERR_CNAMEEXISTS	1807	0x70F	Alias name record exists for the host name
NSERR_INVAL_SVCOPTION	1808	0x710	Option not applicable for this service
NSERR_GSLBBIND_EXISTS	1809	0x711	GSLB binding exists for the given host
NSERR_NOT_LOCALREMOTE	1810	0x712	Site information must be specified for a GSLB service
NSERR_COUNT_MISMATCH	1811	0x713	Address record count does not match the number of services bound to the GSLB vserver
NSERR_IP_MISMATCH	1812	0x714	IP addresses of bound GSLB services and the address records do not match
NSERR_SVCIP_REPEAT	1813	0x715	A GSLB service with the same IP address is already bound to the GSLB vserver
NSERR_NOT_REMOTE	1814	0x716	Service bound to GSLB VIP with -gslb

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
			remote is a local service
NSERR_NOT_LOCAL	1815	0x717	Service bound to GSLB VIP with -gslb local is not a local service
NSERR_PROXY_REC	1816	0x718	A proxy record cannot be assigned to the domain
NSERR_NOPROXY_AREC	1817	0x719	Proxy address records cannot be bound to a GSLB vserver
NSERR_SVC_GSLBBIND_EXISTS	1819	0x71B	GSLB binding exists - unbind the GSLB vserver first
NSERR_SVCTYPEMISMATCH	1820	0x71C	Service type mismatch with existing service/ vserver
NSERR_INVALID_PUBIP_OPTION	1822	0x71E	The public IP and public port are valid only for GSLB local service
NSERR_INVAL_NAME_SYNTAX	1823	0x71F	Invalid domain name syntax
NSERR_GSLB_BACKUP	1824	0x720	Backup VIP is backup of other GSLB VIP. Please unset the existing association and try again

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_IS_BACKUP	1825	0x721	Backup VIP is backup of other VIP. Please unset the existing association and try again
NSERR_GSLB_HAS_BACKUP	1826	0x722	GSLB VIP has a backup. Please unset the backup and try the operation again
NSERR_GSLB_REQUIRES_INDEPENDENT_BACKUP	1827	0x723	Backup VIP to GSLB VIP must not be backup of any other VIP. Please unset the backup and try the operation again
NSERR_GSLB_NO QUALIFIER	1828	0x724	At least one qualifier should be given for the location
NSERR_GSLB_NO NAME	1829	0x725	The qualifier does not exist in the repository
NSERR_GSLB_CUSTOM_NOSPACE	1830	0x726	Too many custom locations
NSERR_GSLB_STATIC_NOSPACE	1836	0x72C	Too many static locations
NSERR_GSLBSITE NAME_EXISTS	1831	0x727	A GSLB site with the same name exists
NSERR_GSLBSITEIP_EXISTS	1832	0x728	A GSLB site with the same IP address exists

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_NO_GSLBSITE	1833	0x729	The GSLB site does not exist
NSERR_LOCAL_EXISTS	1834	0x72A	The local site already exists
NSERR_NO_GSLBSVC	1835	0x72B	The GSLB service does not exist
NSERR_NO_GSLBVIP	1837	0x72D	The GSLB vserver does not exist
NSERR_NO_DMN	1839	0x72F	The domain does not exist
NSERR_DMN_NOT BOUND	1840	0x730	The domain is not bound to this VIP
NSERR_SVCGRP_NOT_SUPPORTED_ON_HEIRARCHICHAL	1841	0x731	GSLB servicegroup is not supported in parent child topology
NSERR_GSLBDOMAIN_BOUND	1842	0x732	The domain is already bound to a GSLB vserver
NSERR_NOT_GSLBENT	1844	0x734	Operation not permitted on a non-GSLB entity
NSERR_GSLBDOMAIN_PERM	1845	0x735	Operation not permitted on a GSLB-configured domain
NSERR_GSLB_MAXQUAL	1846	0x736	Maximum qualifiers allowed is six

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_GSLB_MAXLOCLENGTH	1847	0x737	Maximum allowed location length is 256 characters
NSERR_GSLBVIP_PERM	1848	0x738	Operation not permitted on a GSLB vserver
NSERR_GSLBSVC_PERM	1849	0x739	Operation not permitted on a GSLB service
NSERR_GSLB_MAXSITES	1850	0x73A	Maximum number of sites is 32
NSERR_GSLB_QUALTOOLONG	1851	0x73B	The qualifier is too long
NSERR_GSLB_PERSISTIDEXISTS	1852	0x73C	The persistence ID is already being used by a GSLB vserver
NSERR_GSLB_INVLD_LDNSTO_INTVL	1854	0x73E	Minimum LDNS entry timeout interval is 30 secs
NSERR_VIP_BACKUP_ISGSLB	1856	0x740	GSLB vserver cannot be backup of a non-GSLB vserver
NSERR_GSLB_PUBIP_PUBPORT_EXISTS	1857	0x741	The public IP and public port are being used by another GSLB service
NSERR_GSLBLOCALSVC_ENADIS_NOTALLOWED	1858	0x742	GSLB local service status not changed - please enable or disable the

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
			corresponding LB vserver instead
NSERR_GSLBLOCALSVR_ENADIS_NOTALLOWED	1859	0x743	Server status not changed - the server has a GSLB local service
NSERR_INVALID_PERSISTID	1860	0x744	Invalid persistence ID
NSERR_PERM_PERSISTID	1861	0x745	The persistence ID is required for persistence or spillover-persistency to be set
NSERR_INVALID_LOCALSITEIP	1862	0x746	Invalid GSLB local site IP address
NSERR_INVALID_REMOTESITEIP	1863	0x747	Invalid GSLB remote site IP address
NSERR_INVALID_SITETYPE	1864	0x748	Invalid GSLB site type
NSERR_INVALID_BACKUPIP	1865	0x749	Invalid backup IP for the GSLB domain
NSERR_GSLBVIP_MAXSVC	1866	0x74A	Cannot bind more than 32 services to a GSLB vserver
NSERR_INVALID_JITTER	1867	0x74B	RTT tolerance value must be between 1 and 100
NSERR_GSLBLOCSVC_DIS_NOTALLOWD	1868	0x74C	Cannot add GSLB local service with state set to DISABLED

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_DUMMYBKUP_NOTALLOWD	1869	0x74D	A backup vserver with no IP address and port must be of type GSLB
NSERR_GSLBSVC_BIND_NOTALLOWD	1870	0x74E	Cannot bind GSLB service to a vserver with valid IP and port
NSERR_NSMAP_VERSION	1871	0x74F	Unrecognized NetScaler file version
NSERR_NSMAP_FORMAT	1872	0x750	Unrecognized file format specified
NSERR_NSMAP_EOF	1873	0x751	End of file has been reached
NSERR_NSMAP_PARSE	1874	0x752	File parsing error
NSERR_NSMAP_READ	1875	0x753	Error reading file
NSERR_NSMAP_CHILD_FORK_FAILED	1876	0x754	Child process creation failed
NSERR_NSMAP_NOSPACE	1877	0x755	No space left in /var/ disk partition. Free up some space and retry
NSERR_NSMAP_OUTPUTFILE	1878	0x756	Error opening output file for writing
NSERR_NSMAP_INPUTFILE	1879	0x757	Error opening input file for reading

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_NSMAP_REQUIRED_FIELD	1880	0x758	Required field missing
NSERR_NSMAP_DBFILE	1881	0x759	Error opening database file
NSERR_NSMAP_DBINSERT	1882	0x75A	Error inserting entry into the database
NSERR_NSMAP_DBSEARCH	1883	0x75B	Error searching the database
NSERR_GSLBPROXM_LICENCE_ABSENT	1884	0x75C	Cannot set proximity methods without GSLB proximity license
NSERR_GSLB_SITEPERSISTENCE_HTTPONLY	1885	0x75D	Site persistence is valid only for HTTP or SSL GSLB services
NSERR_GSLB_NOSITEPFX	1886	0x75E	Site prefix compulsory if site persistence is HTTPRedirect
NSERR_GSLB_SITEPREFIX_SIZE	1888	0x760	Site prefix size exceeds maximum
NSERR_GSLB_SITEDOMAIN_SIZE	1889	0x761	Site domain cannot be created - name length exceeds maximum
NSERR_GSLB_SITEDOMAIN_SYNTAX	1890	0x762	Site domain cannot be created - name is invalid

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_GSLB_SITEDOMAIN_REFERS	1891	0x763	Site domain cannot be deleted - it has external DNS references
NSERR_GSLBDOMAIN_REFERS	1892	0x764	GSLB domain cannot be deleted - it has external DNS references
NSERR_GSLB_ARECORD_EXISTS	1893	0x765	GSLB record cannot be created - another A record is configured with the same name
NSERR_GSLB_SITECOOKIE_TIMEOUT_RANGE	1894	0x766	Invalid GSLB site cookie timeout
NSERR_GSLBDOMAIN_SYNTAX	1895	0x767	GSLB domain cannot be created - name is invalid
NSERR_GSLB_SO_PERM	1896	0x768	Spill-over cannot be set on a GSLB vserver
NSERR_GSLB_DEPRCOOKIETOUT	1897	0x769	Ignored deprecated cookietimeout setting since it has been made a per-domain configuration
NSERR_DNS_NAMESVR_SYNTAX	1898	0x76a	Invalid name server syntax
NSERR_DNS_ORIGSVR_SYNTAX	1899	0x76b	Invalid origin server syntax

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_DNS_CONTACT_SYNTAX	1900	0x76c	Invalid contact name syntax
NSERR_DNS_MX_SYNTAX	1901	0x76d	Invalid mail exchange syntax
NSERR_DNS_CNAME_SYNTAX	1902	0x76e	Invalid canonical name syntax
NSERR_DNS_ALIAS_SYNTAX	1904	0x770	Invalid alias name syntax
NSERR_GSLB_NOLOCALVIP	1905	0x771	Cannot create GSLB local service - add the local vserver first
NSERR_GSLB_LOCALSVCEXISTS	1906	0x772	Cannot delete the vserver - corresponding GSLB local service still exists
NSERR_GSLBLOCALSVC_PERM	1907	0x773	Operation not permitted on GSLB local service
NSERR_DNS_INVAL_REVDOMNAME_SYNTAX	1908	0x774	Invalid reverse domain name syntax
NSERR_DNS_ALIASREC	1909	0x775	Alias name cannot have any record
NSERR_GSLBLOCSVC_DELAYEDCLEAN_NOTALLOWD	1910	0x776	Down state flush cannot be set on GSLB local service
NSERR_NO_BKP_VIP	1911	0x777	Set a backup Vserver, to enable it.

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_GSLB_NOSUCH_LDNSENTRY	1912	0x778	LDNS entry does not present
NSERR_MAX_DNS_VIEW	1913	0x779	Number of DNS views exceeds limit
NSERR_GSLB_SITE_IP_EXISTS	1914	0x77a	GSLB Site IP already exists
NSERR_GSLB_LAST_MIP	1915	0x77b	MIP is not removed. At least one MIP is required
NSERR_RM_GSLB_SITE	1916	0x77c	IP cannot be removed as it is being used by the GSLB local site
NSERR_GSLB_IPRM_LAST_MIP	1917	0x77d	GSLB Site IP removed. MIP is not removed. At least one MIP is required
NSERR_GSLB_SVC_PUB_PORT_ERR	1918	0x77e	Cannot modify public port for remote GSLB service/ service item
NSERR_REC_HAS_REF	1919	0x77f	DNS record has references
NSERR_DNS_VIEW_REF	1920	0x780	The dns view cannot be removed as it has dependencies
NSERR_GSLB_SITE_PERSISTENCE_MATCH	1921	0x781	Mismatch in gslb site persistence type with other bound services

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_GSLB_SITE_PERSISTENCE_CONFLICTS	1922	0x782	Site persistence conflicts with other services/ servicegroups bound to the gslb vserver(s)
NSERR_DNS_POLICY_INVAL	1923	0x783	Invalid DNS policy
NSERR_GSLBVIP_CNAME_MISMATCH	1924	0x784	GSLB vserver cannot be bound with cname based and ip based services at the same time
NSERR_GSLBVIP_CNAME_UNSUPPORTED_LBMETHODS	1925	0x785	GSLB vserver having cname services cannot have dynamic load balancing methods
NSERR_GSLB_SERVICE_MON_NOIPPORT	1926	0x786	Cannot bind monitor with zero ip or port to a cname gslb service
NSERR_GSLB_SERVICE_MON_SET_NOIPPORT	1927	0x787	Cannot set ip or port to zero when monitor is bound to a cname gslb service.
NSERR_GSLB_CNAME_SERVICE_SET	1928	0x788	Setting of these parameters on cname gslb service is not allowed
NSERR_GSLB_CNAME_VSERVER_SET	1929	0x789	Setting of these parameters on gslb vserver having

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
			cname services is not allowed
NSERR_GSLBVIP_CNAME_UNSUPPORTED_BKUP_LBMETHODS	1930	0x78a	GSLB vserver having cname services cannot have dynamic backup load balancing methods
NSERR_GSLBVIP_CNAME_UNSUPPORTED_EDR	1931	0x78b	GSLB vserver having cname services cannot have empty down response disabled
NSERR_GSLBVIP_CNAME_UNSUPPORTED_MIR	1932	0x78c	GSLB vserver having cname services cannot have multiple ip response enabled
NSERR_GSLBSVC_VIEW_NEXIST	1933	0x78d	View is not bound to the GSLB service
NSERR_DNS_TTL_MORE_THAN_MAX_ALLOWED	1934	0x78e	DNS RECORD TTL value greater than max TTL allowed
NSERR_GSLB_LB_MAXSITES	1935	0x78f	Maximum number of LB sites is 1024
NSERR_GSLB_HASCHILDREN	1936	0x790	Cannot remove site that has child site(s)
NSERR_GSLB_PARENTISCHILD	1937	0x791	Parent site cannot be a child to another site
NSERR_MAX_STREAM_SELECTORS	1938	0x792	Number of selectors exceeds limit

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_MAX_STREAM_IDENTIFERS	1939	0x793	Number of identifiers exceeds limit
NSERR_NO_SUCH_SELECTOR	1940	0x794	The given selector does not exist
NSERR_NO_SUCH_IDENTIFIER	1941	0x795	The given identifier does not exist
NSERR_RLT_TIMESLICE_INVALID_VAL	1942	0x796	Time slice should be a multiple of 10
NSERR_ILLEGAL_SUBNET_MASK	1943	0x797	Incorrect subnet mask value
NSERR_STREAM_SELECTOR_INUSE	1944	0x798	The selector is being referenced by one or more identifiers
NSERR_IDENTIFIER_INUSE	1945	0x799	The identifier is being referenced by one or more policies
NSERR_SELECTOR_CANNOT_CHANGE_ATTRIB_TYPE	1946	0x79A	Cannot change request type selector to response type
NSERR_GSLB_IGN_TRIGMON	1947	0x79B	Trigger monitor setting assumed ALWAYS for GSLB local site
NSERR_SELECTOR_NOT_MORE_THAN_2_IPV6_EXP	1948	0x79C	Cannot exceed more than two IPV6 expressions in a selector
NSERR_REPEATED_MONITORS	1949	0x79D	Monitors cannot be repeated

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_ALL_MONITORS_DISABLED	1950	0x79E	All monitors in selected list are disabled.
NSERR_GSLB_AAAARECORD_EXISTS	1951	0x79F	GSLB record cannot be created - another AAAA record is configured with the same name
NSERR_GSLBVIP_HETEROGENEOUS_SERVICE_IPVERSION	1952	0x7A0	Heterogeneous service/servicegroup binding is not allowed for GSLB vserver
NSERR_VIEWIP_IPV6	1953	0x7A1	View IP setting is not allowed for IPv6 GSLB service.
NSERR_BACKUPIP_IPV6	1954	0x7A2	IPv4 backup IP setting is not allowed for IPv6 GSLB vserver.
NSERR_BACKUP_VIP_MISMATCH	1955	0x7A3	Both primary and secondary vservers should be of same DNSRecordType
NSERR_GSLB_DOMAIN_CONVERSION	1956	0x7A4	Cannot associate gslb domain to the service.
NSERR_GSLB_IPV4_BACKUPIP	1957	0x7A5	IPv6 service binding is not allowed along with IPv4 backup IP.
NSERR_CANNOT_ADD_SELECTOR	1958	0x7A6	Cannot set a new selector when the identifier with no

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
			selector is bound to a policy.
NSERR_SEL_CONFLICTING_ATTRIBUTES	1959	0x7A7	Conflicting attributes in the new and current selector sets.
NSERR_GSLBVIP_CNAME_BACKUPIP	1960	0x7A8	GSLB vserver having cname services cannot have backup IP
NSERR_GSLB_HETEROGENEOUS_SITEIP	1961	0x7A9	Heterogeneous IPv6 and IPv4 GSLB site IPs not allowed.
NSERR_DNS_MAX_AAAA_REC	1962	0x7AA	Cannot exceed more than 5 IPv6 addresses.
NSERR_DNS_MAX_A_REC	1963	0x7AB	Cannot exceed more than 25 IP addresses.
NSERR_GSLB_RECTYPE_SERVICE	1965	0x7AD	Cannot set the record type while services/ servicegroups are bound to the GSLB vserver.
NSERR_GSLB_RECTYPE_DOMAIN	1966	0x7AE	Cannot set the record type while domains bound to the GSLB vserver.
NSERR_GSLB_RECTYPE_BACKUP_VIP	1967	0x7AF	Cannot set the record type while GSLB vserver has backup vserver.

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_GSLB_BKPVIP_RECTYPE	1968	0x7B0	Cannot set the record type while GSLB vserver is a backup vserver.
NSERR_GSLBVIP_NAPTR_UNSUPPORTED_SVCTYPE	1969	0x7B1	GSLB vserver of NAPTR DNS record type can have only ANY as service type.
NSERR_BACKUPIP_IPV4	1970	0x7B2	IPv6 backup IP setting is not allowed for IPv4 GSLB vserver.
NSERR_GSLB_IPV6_BACKUPIP	1971	0x7B3	IPv4 service binding is not allowed along with IPv6 backup IP.
NSERR_GSLB_DB_REQ_TOO_BIG	1972	0x7B4	Static proximity Database request is too big.
NSERR_GSLB_DB_QUEUE_MAXED	1973	0x7B5	Static proximity Database queue is full.
NSERR_GSLB_DB_SERVER	1974	0x7B6	Static proximity database server is not running.
NSERR_GSLB_DB_TIMEOUT	1975	0x7B7	Static proximity database server is not responding.
NSERR_GSLB_DB_CLOSED	1976	0x7B8	Connection to static proximity database server is closed.

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_GSLB_COORDINATES	1977	0x7B9	Both longitude and latitude should be specified or not.
NSERR_INVALID_IPV6_PREFIXLEN	1978	0x7BA	Invalid IPv6 prefix length.
NSERR_GSLBDOMAIN_CANME_RECORD_EXISTS	1979	0x7BB	Cname record can't be created. Another record exists for the configured domain.
NSERR_GSLBDOMAIN_AAAA_CNAME_EXISTS	1980	0x7BC	Cname record exists for the configured domain.
NSERR_GSLB_NON_PARENT_REMOTESITE	1981	0x7BD	Cannot have a gslb remote site, other than the parent site, configured on an LB node
NSERR_ZONE_EXISTS	1982	0x7BE	Zone already configured.
NSERR_INVAL_KEYFLAGS	1983	0x7BF	Invalid flags value in DNSKEY
NSERR_DNSKEY_NONEXISTS	1984	0x7C0	Zone has no DNSKEY's
NSERR_NORECS_IN_ZONE	1985	0x7C1	No records in zone
NSERR_SIGNFAILED	1986	0x7C2	RSA Sign operation returned error
NSERR_DIGESTINIT_FAILED	1987	0x7C3	Digest init before RSA Sign operation returned error

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_DIGESTUPDATE_FAILED	1988	0x7C4	Digest update before RSA Sign operation returned error
NSERR_KEYEXISTS	1989	0x7C5	The DNSKEY is already added for this zone
NSERR_NOPASVKEYS	1990	0x7C6	No Passive DNSKEY's in zone
NSERR_DNS_MAXKEYSIZE	1991	0x7C7	Maximum allowed public key size is 1024 and private key size is 4096
NSERR_NODATA_TO_SIGN	1992	0x7c8	No data to sign the record
NSERR_CNAME_SITE_NOTEXISTS	1993	0x7c9	Site name must be specified for cname based GSLB service.
NSERR_DNS_NOSOA_NONS	1994	0x7cA	No SOA or NS records for the zone
NSERR_DNS_PROXY_ZONE	1995	0x7cB	Cannot sign/unsign a proxy zone
NSERR_NOACTVKEYS	1996	0x7CC	No active DNSKEY's in zone
NSERR_NOTIFYPERIOD	1997	0x7cd	Notification period must be less than the expiry period
NSERR_LOAD_PUBKEY	1998	0x7ce	Public key loading failed

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_DNSKEYGEN_UNSUPPORTED_ALGO	1999	0x7cf	Unsupported algorithm
NSERR_DNSKEYGEN_ERR_PUBFILE_OPEN	2000	0x7d0	Error opening public key file
NSERR_DNSKEYGEN_ERR_PRIVFILE_OPEN	2001	0x7d1	Error opening private key file
NSERR_DNSKEYGEN_ERR_DSFILE_OPEN	2002	0x7d2	Error opening delegation signer (DS) file
NSERR_GSLB_OPT_NOTSUPPORTED	2003	0x7d3	gslb option is not supported, GSLB site is mandatory for GSLB services
NSERR_GSLB_GFS_NOT_SUPPORTED	2004	0x7d4	Graceful shutdown is not supported for GSLB services.
NSERR_NSMAP_IMPORTFILE	2005	0x7d5	Error reading the imported file. See /var/log/ns.log file for more details.
NSERR_DNS_CNAMELOOP	2006	0x7d6	Addition of this CNAME record leads to a CNAME loop
NSERR_NEWSVC_NOT_4GSLB	2007	0x7d7	startup settings not applicable to GSLB vservers

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_NON_CLUSTER_SYSTEM	2008	0x7d8	The option is only supported for clustering systems.
NSERR_PM_MON_NOT_ENABLED	2009	0x7d9	Path monitoring must be enabled to enable this option.
NSERR_GSLB_BACKUP_PERS_DEPRICATED	2010	0x7dA	GSLB Backup Persistence is deprecated. Please use Spillover Persistence instead.
NSERR_DNS_SIGNFAIL	2011	0x7dB	DNSSEC Sign operation failed
NSERR_DNS_NEED_PROXY	2012	0x7dC	Zone needs to be in proxy mode
NSERR_DNSSEC_OFFLOAD_NOSUPPORT	2013	0x7dD	DNNSEC Offload is not supported in this platform.
NSERR_DNS64_ACT_INVAL	2014	0x7dE	Invalid DNS64 action.
NSERR_DNS64_NOT_SUPPORTED_VS	2015	0x7dF	Specified policy can be bound only to DNS/DNS_TCP vserver.
NSERR_DNS64_INVAL_PREFIX	2016	0x7e0	Specified Prefix is either not allowed or Prefix length is not in [96, 64, 56, 48, 40, 32].

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_GSLB_DB_REPEAT_REQUEST	2017	0x7e1	Location database request need to be repeated
NSERR_GSLBSITE_CONN_NOTSUPPORTED	2018	0x7e2	This may cause GSLB site MEP connection issues in some earlier releases.
NSERR_DNS64_TIMEOUT_ROUNDOFF	2019	0x7e3	Timeout threshold is rounded off to nearest multiple of 10 less than the given value.
NSERR_GSLB_SITE_PREFIX_CONFLICT	2044	0x7fc	Site prefix conflicts with another service bound to the gslb vip
NSERR_DNSKEY_MISMATCH	2024	0x7e8	The Key specified is not valid for this zone
NSERR_INVALID_REMOTE_CLIP	2025	0x7e9	Invalid remote GSLB site CLIP. CLIP belong to the local gslb site
NSERR_IPV6_CLIP_NOTSUPPORTED	2026	0x7ea	IPV6 CLIP is not supported
NSERR_NON_DEFAULT_DBFILE_LOC	2027	0x7eb	In case of HA setup and cluster system, the command might fail on other nodes if an identical copy of the file is not present at the same location.

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_LOC64_FROM_TO_TYPE	2028	0x7ec	IP From and IP To in location specification are of different IP type.
NSERR_DNS_NOSOA_NONS_ZONE_NO_PROXY_MODE	2029	0x7ed	Cannot delete SOA or NS records for a zone that is not deployed in proxy mode.
NSERR_DNS_ACTION_DROP_DEPRECATED	2031	0x7ef	Drop is deprecated. Please use Drop action type under Responder feature.
NSERR_DNS_ACTION_REWRITE_RESPONSE_DEPRECATED	2039	0x7f7	Rewrite Response is deprecated. Please use replace_dns_answer_section action type under Rewrite feature.
NSERR_IDENTIFIER_INVAL_THRESHOLD	2040	0x7f8	Stream Identifier min and max threshold cannot both be zero and min threshold cannot be greater than max threshold
NSERR_IDENTIFIER_INVAL_SORT	2041	0x7f9	Stream Identifier sort option is invalid
NSERR_NO_SUCH_DNSPROF	2042	0x7fa	DNS profile does not exist
NSERR_DNS_PROFILE_SVC_TYPE	2043	0x7fb	DNS profile cannot be set to this service type

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_CSGSLB_POLICY_SET_NOTALLOWED	2046	0x7fe	Policy bound to CS GSLB vserver must have a gslb targetvserver
NSERR_CS_POLICY_SET_NOTALLOWED	2045	0x7fd	Policy bound to non CS GSLB vserver must not have a gslb targetvserver
NSERR_GSLB_ECS_DISABLED_VALIDATION_ENABLED	2987	0xbab	ECS is disabled: Enabling only ECS address validation will not have any effect if ECS is not enabled.
NSERR_ECS_INVALID_ADDR_LEN	2989	0xbad	ECS address uses more octets than required or the address has non-zero bits set beyond SOURCE PREFIX-LENGTH
NSERR_GSLB_ECS_MIR_BOTH_SET	765	0x2fd	ECS option is mutually exclusive with MIR
NSERR_GSLB_ECS_IPV6_DISABLED	766	0x2fe	IPv6PT is disabled, DNS queries with an IPv6 ECS address will be dropped
NSERR_GSLB_ECS_LBMETHOD_NOT_SP	767	0x2ff	Enabling ECS without setting LB method to Static Proximity will not result in optimal

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
			responses for ECS-enabled queries
NSERR_REM_FAIL_NOMEM	1499	0x5DB	Removal is unsuccessful because of an internal error
NSERR_GSLB_MEP_KEEP_ALIVE_LOW_TIMEOUT	1802	0x70A	Provided MEPKeepAliveTimeout value is less than 4 seconds that might lead to frequent MEP flaps.
NSERR_GSLB_MEP_KEEP_ALIVE_TIMEOUT	1803	0x70B	Same value of MEPKeepAliveTimeout should be configured in all GSLB nodes including Child GSLB nodes for optimum behaviour.
NSERR_GSLB_SYNC_INT_PART_WARN	1804	0x70C	Changing GSLB sync interval from non-default partition will have no effect.
NSERR_GSLB_SYNC_INT_NONPART_WARN	1805	0x70D	For changing the GSLB sync interval in a partition setup, this command needs to be fired manually on all GSLB nodes.
NSERR_INVAL_CAA_TAG	2320	0x910	Invalid CAA record tag syntax.

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_GSLB_ISNOTCHILD	2349	0x92D	Parent site cannot be changed if the site is not already a child site
NSERR_GSLB_PARENT_CHANGE_ON_CHILD	2350	0x92E	Parent change not accepted on the child site. Change the name and the ip of the parent instead
NSERR_ADDRINUSE_BY_VSERVER	2351	0x92F	Address already in use by a VServer

GSLB2 ERRORS

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_DNS_VIEW_NOENT	3008	0xbc0	DNS View does not exist
NSERR_GSLB_LOC_NOMEM	3009	0xbc1	Memory allocation for location failed.
NSERR_DNS_PRIO_INVAL_VALUE	3010	0xbc2	Cannot bind DNS Policy with priority > 65535
NSERR_DNSPROF_EXISTS	3011	0xbc3	DNS Profile already exists.
NSERR_DNSPROF_DEF	3012	0xbc4	Cannot remove default DNS Profile.
NSERR_GSLB_LOC_EXISTS	3013	0xbc5	Custom Location Overlaps with an already existing location.

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_GSLB_LOC_NOENT	3014	0xbc6	Custom Location does not exist.
NSERR_GSLB_NOMEM	3015	0xbc7	Not enough memory for GSLB operation.
NSERR_DNS_INT_POL	3016	0xbc8	Internal Policy is not allowed to bind if builtin parameter is not set with any value.
NSERR_GSLB_MEP	3017	0xbc9	Cannot enable MEP (Network Metric / Persistency Exchange) on a Child Site.
NSERR_IP_ROUTE_EXISTS	3018	0xbca	Host route enabled on this IP, cannot be used for GSLB Site IP.
NSERR_DNS_VIEW_EXISTS	3019	0xbcb	DNS View already exists
NSERR_NAME_VSVR_PERM	3020	0xbcc	Operation not permitted on a Vserver based Nameserver.
NSERR_DNS_POL_INTERNAL	3021	0xbcd	Cannot remove or unbind internal DNS policy
NSERR_DNS_NOMEM	3022	0xbce	Not enough memory for DNS Operation
NSERR_GSLB_NAPTR_SERVICE_SET	3023	0xbcf	Setting of these parameters on naptr

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
			gslb service is not allowed
NSERR_GSLB_NAPTR_REPLACEMENT_UNSET	3025	0xbd1	Unsetting of naptr replacement is not allowed if the gslb service is bound to gslb vserver of NAPTR dnsrectype.
NSERR_GSLBVIP_NAPTR_UNSUPPORTED_LBMETHODS	3026	0xbd2	GSLB vserver having NAPTR services can have only CUSTOM LOAD as lb method.
NSERR_GSLB_NAPTR_VSERVER_SET	3027	0xbd3	Setting of these parameters on natpr gslb vserver is not allowed.
NSERR_GSLB_NAPTR_DOMAIN_SIZE	3028	0xbd4	NAPTR domain cannot be created - name length exceeds maximum
NSERR_GSLB_NAPTR_DOMAIN_SYNTAX	3029	0xbd5	NAPTR domain cannot be created - name is invalid
NSERR_GSLB_NAPTR_REPLACEMENT_SUFFIX_SYNTAX	3030	0xbd6	Invalid NATPR Replacement Suffix
NSERR_GSLB_NON_NAPTR_SERVICE	3031	0xbd7	Operation permitted only on NAPTR GSLB service
NSERR_GSLB_USE_FORCESYNC	3032	0xbd8	Force sync option must be used in the 'sync gslb config' command to

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
			synchronize the configuration to other GSLB sites, or manually add the requisite configuration to other sites.
NSERR_INVALID_WILDCARD_CONFIG	3033	0xbd9	Invalid Wildcard Configuration
NSERR_GSLB_SYNC_SAVECMD_WARN	3034	0xBDA	Saveconfig command might not get applied to GSLB sites which are down during the sync operation, so it is recommended to apply saveconfig on master node again when down gslb sites comes up.

ICA CLIENT VERSION ERRORS

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_ICA_CLIENT_VERSION_UNKNOWN_CLIENT_TYPE	3536	0xdd0	Unknown ICA client type.
NSERR_ICA_CLIENT_VERSION_DEFAULT_WHITELISTING	3537	0xdd1	Failed to initialize the ICA whitelist: Switched to default static ICA whitelisting
NSERR_ICA_CLIENT_VERSION_NOT_	3538	0xdd2	The ICA client version you are

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
FOUND_IN_EXCEPTION_LIST			requesting to remove from the exception list is not present in the exception list.
NSERR_ICA_CLIENT_VERSION_INCORRECT_BASE_VERSION_FORMAT	3539	0xdd3	Invalid format for the ICA client base version entered.
NSERR_ICA_CLIENT_VERSION_INCORRECT_EXCEPTION_LIST_FORMAT	3540	0xdd4	Invalid format for the ICA exception list entered.
NSERR_ICA_CLIENT_VERSION_DUPLICATES_RECEIVED_TO_REMOVE	3541	0xdd5	Two or more of the same client versions entered in the ICA exception list.

ICA LATENCY PROFILE ERRORS

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_ICA_LATENCY_PROFILE_ACTIVE_CONNECTIONS	3542	0xdd6	Cannot remove the Latency profile as there are active ICA connections associated with this profile.

INAT ERRORS

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_PUBLICIP	3888	0xf30	Invalid Public IP address

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_PRIVATEIP	3889	0xf31	Invalid Private IP address
NSERR_PROXYIP	3890	0xf32	Invalid Proxy IP address
NSERR_WILDCARD TCPVIP	3891	0xf33	TCPPROXY enabled INAT and wildcard TCP Vserver not allowed
NSERR_WILDCARD ANYVIP	3892	0xf34	INAT rule and wildcard ANY vserver, not allowed
NSERR_FTPVIPPR ESENT	3893	0xf35	FTP enabled INAT and FTP vserver not allowed
NSERR_V46_USIP	3894	0xf36	USIP is not allowed in mixed topology
NSERR_INCOMPAT IBLE_IP	3895	0xf37	Private and Proxy IP should share the same IP Type
NSERR_ONLY_NAT 46_SUPPORTED	3896	0xf38	Stateless mode only supported for IPv4->IPV6
NSERR_NAT46_PR OXY_IP	3897	0xf39	Proxy IP is not supported in stateless mode
NSERR_NAT46_INV ALID_PREFIXLEN	3898	0xf3A	Prefix length should be 32/40/48/56/64/96
NSERR_NAT46_INV ALID_SETTING	3899	0xf3B	Invalid configuration for nat46

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_NAT46_PRIVATEIP_EXISTS	3900	0xf3C	Private IP already configured in another nat46 rule
NSERR_TFTPVIPPRESENT	3901	0xf3d	TFTP enabled INAT and TFTP vserver not allowed
NSERR_SETUNSETINAT_NOTSUPPORTED	3902	0xf3E	Setting and Unsetting mode of INAT not supported

INTERNAL NAMESERVER ERRORS

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_NAME_SVR_EXISTS	2561	0xa01	Name server already exists.
NSERR_NAME_SVR_IDNS_NEMPTY	2562	0xa02	Name servers already configured.
NSERR_NAME_SVR_IVALPOLICY	2563	0xa03	Invalid LB method for vserver-based name server.
NSERR_NAME_SVR_IVALPROTO	2564	0xa04	Invalid service type for vserver-based name server.
NSERR_NAME_SVR_ADD_NEXIST_VIP	2565	0xa05	vserver does not exist.
NSERR_NAME_SVR_NEXIST	2566	0xa06	Name server does not exist.
NSERR_NAME_SVR_IDNS_PERM	2567	0xa07	Operation on internal entity not permitted

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_NAME_SVR_IP_EXISTS	2568	0xa08	Name server exists with this IP address
NSERR_NAME_SVR_TYPE_NEXIST_VIP	2569	0xa09	vserver of given type does not exist.
NSERR_NAME_SVR_INVAL_PROTOTYPE	2570	0xa0a	Invalid protocol type for local nameserver.
NSERR_NAME_SVR_DYN_VSRVR_EXISTS	2571	0xa0b	Dynamic vserver of same type exists.

INTF ERRORS

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_1GSFPSPEEDLIMIT	3968	0xf80	1G SFP's are restricted to speed 1000 or AUTO only
NSERR_1GSFPDUPLEXLIMIT	3969	0xf81	1G SFP's are restricted to duplex FULL or AUTO only
NSERR_1GSPEEDLIMIT	3970	0xf82	1G port can not be configured as 10G speed
NSERR_1GDUPLEXLIMIT	3971	0xf83	1G port can not be configured as HALF duplex
NSERR_10GSPEEDLIMIT	3972	0xf84	10G ports on this platform can only be configured as speed

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
			1G, 10G or AUTO only
NSERR_10GDUPLEXLIMIT	3973	0xf85	10G ports on this platform can only be configured as duplex FULL or AUTO only
NSERR_10GAUTONEGLIMIT	3974	0xf86	10G ports on this platform do not support AUTONEG
NSERR_10GSPEEDONLY	3975	0xf87	10G ports on this platform are restricted to speed 10000 or AUTO only
NSERR_FULLDUPLEXONLY	3976	0xf88	These ports do not support HALF duplex mode
NSERR_AUTOINVALSPEED	3977	0xf89	Static CLAG does not support speed as AUTO
NSERR_CLAGSPEEDREQ	3978	0xf8a	Static CLAG explicitly requires speed to be configured other than AUTO
NSERR_THROUGHPUTLIMIT	3979	0xf8b	Throughput limit error. Possible values: 1G port - 1000Mbps, 10G port - 10000Mbps, 40G port - 40000Mbps, Link Aggregation - 80000Mbps

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_BANDWIDTHLIMIT	3980	0xf8c	Bandwidth limit error. Possible values: 1G port - 1000Mbps, 10G port - 10000Mbps, 40G port - 40000Mbps, Link Aggregation - 80000Mbps
NSERR_10GDAC_SPEEDLIMIT	3981	0xf8d	DAC port speed must be configured as 10G or AUTO
NSERR_VIF_LACP_CAUTION	3982	0xf8e	Ensure that the physical interface is not shared with any other VMs.
NSERR_LA_SLAVE_LIMIT	3983	0xf8f	Trying to bind more interfaces than allowed limit
NSERR_SLAVE_MTU_MISMATCH	3987	0xf93	Interface MTU should be same as Channel MTU.
NSERR_BKPLANE_MTU_MISMATCH	3988	0xf94	Interface MTU should be default or same as Backplane MTU.
NSERR_MTU_NOT ALLOWED	3989	0xf95	MTU change is not allowed on this interface.
NSERR_BACKPLANE_MTU_LIMIT	3990	0xf96	Backplane Interface, Minimum user configured value for MTU is 1579.

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_INTERFACE_SLAVE_MTU_LIMIT	3991	0xf97	Interface is a part of channel, MTU change is not allowed.
NSERR_CHANNEL_RESTRICT	447	0x1BF	LA channel configuration on VPX running on SDX should be done only from Service VM
NSERR_PTP_CLUS_L3	3992	0xf98	Cluster INC Mode Enabled, PTP state change is not allowed.
NSERR_40GDUPLEXLIMIT	3993	0xf99	40G ports on this platform can only be configured as duplex FULL or AUTO only
NSERR_40GSPEEDONLY	3994	0xf9a	40G ports on this platform are restricted to speed 40000 or AUTO only
NSERR_LRSET_FC_NOT_ALLOWED	3996	0xf9c	Flow Control settings not allowed for link redundant set interface
NSERR_LRSET_LACP_SET_NOT_ALLOWED	3997	0xf9d	Dynamic LA(LACP) settings are not allowed for link redundant set interface
NSERR_LRSET_LLDPSET_NOT_ALLOWED	3998	0xf9e	LLDP settings are not allowed for link

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
			redundant set interface
NSERR_LRSET_SPEED_NOT_ALLOWED	3999	0xf9f	speed setting not allowed for link redundant set interface
NSERR_LRSET_PRIORITY_NOT_ALLOWED	4026	0xfba	lrset priority not allowed for link redundant set master interface
NSERR_LRSET_THROUGHPUT_NOT_ALLOWED	4027	0xfbb	throughput setting not allowed for link redundant set master interface
NSERR_LRSET_BW_SET_NOT_ALLOWED	4028	0xfbc	Bandwidth settings are not allowed for link redundant set interface
NSERR_LRSET_LAG_TYPE_NOT_ALLOWED	4029	0xfbd	Lagtype setting not allowed for link redundant set interface
NSERR_LRSET_DUPLEX_NOT_ALLOWED	4030	0xfbe	Duplex setting not allowed for link redundant set interface
NSERR_LRSET_AUTO_NEG_NOT_ALLOWED	4031	0xfbf	Disabling autonegotiation not allowed for link redundant set interface
NSERR_JF_ESX_VERSION_SUPPORT	4070	0xfe6	Jumbo Frames are supported on ESX

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
			5.5 version and onward
NSERR_TP_SETTINGS_NOT_ALLOWED	3385	0xd39	Trunk Port settings on this interface is not supported
NSERR_LACP_SETTINGS_ON_TP_NOT_ALLOWED	3386	0xd3a	LACP settings on Trunk Port is not allowed
NSERR_IP6_ADDRESS_SETTING_FAILED	3387	0xd3b	IPv6 Address can not be added because MTA table got exhausted
NSERR_50GSPEEDLIMIT	3388	0xd3c	50G ports on this platform can only be configured as speed 10G, 25G, 40G(except MPX-92XX and MPX-17XXX), 50G or AUTO
NSERR_100GSPEEDLIMIT	3389	0xd3d	100G ports on this platform can only be configured as speed 10G, 25G, 40G, 50G, 100G or AUTO
NSERR_RX_RINGSIZE_CHANGE_NOTALLOWED	2289	0x8f1	Ringsize change is not allowed on this NIC type.
NSERR_RX_RINGSIZE_INVALID	2290	0x8f2	Receive ringsize is invalid.
NSERR_RX_RINGTYPE_CHANGE_NOTALLOWED	2291	0x8f3	Receive ringtype change is not

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
			allowed on this NIC type.
NSERR_INTERFACE_LOOPBACK	2292	0x8f4	Operation not allowed on loopback interface.
NSERR_INTERFACE_INTERNAL	2293	0x8f5	Operation not allowed on internal interface.
NSERR_RX_RINGTYPE_SAVE	2295	0x8f7	Save the ring size to loader.conf file.
NSERR_200GSPEEDLIMIT	2296	0x8f8	200G ports on this platform can only be configured as speed 10G, 25G, 40G, 50G, 100G, 200G or AUTO

JAZZ ERRORS

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_BO_LAC_NOT_FOUND	3409	0xd51	Make sure that you have entered a valid License Access Code. Note that licenses can also be allocated in My Account on Citrix.com. For assistance, contact Citrix Customer Service
NSERR_JBOC_FAILED	3410	0xd52	License files cannot be saved. You must

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
			select a different directory or edit the permissions for this directory.
NSERR_BO_SESSION_EXPIRED	3411	0xd53	Your session has expired.
NSERR_BO_LAC_FULLY_ALLOCATED	3412	0xd54	All available licenses have been allocated for this License Access Code. Enter a different code or contact Citrix Customer Service.
NSERR_BO_WEBKEY_NOT_SUPPORTED	85	0x55	This license cannot be allocated automatically. To allocate it manually, go to My Account on Citrix.com
NSERR_JBOC_CITRIX_RESPONSE	3414	0xd56	This operation could not be completed. If you are trying to allocate a license, go to My Account on Citrix.com. For assistance, contact Citrix Customer Service.
NSERR_JBOC_CITRIX_CONNECTION_FAILED	3415	0xd57	There is a network connection issue. Please try again later or go to My Account on Citrix.com

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_BO_GENERIC	3416	0xd58	Your request could not be completed due to an error. Please contact Citrix support
NSERR_BO_SN_NOT_FOUND	3417	0xd59	Make sure that you have entered a valid Serial Number. Note that licenses can also be allocated in My Account on Citrix.com. For assistance, contact Citrix Customer Service

LB ERRORS

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_SLESSLB_LBMETHOD_NOTSUPPORTED	1280	0x500	Incompatible LB method for sessionless vserver
NSERR_SLESSLB_PERSIST_NOTSUPPORTED	1281	0x501	Incompatible persistence method for sessionless vserver
NSERR_SLESSLB_TYPE_NOTSUPPORTED	1282	0x502	Sessionless vserver must be of type ANY, DNS or UDP
NSERR_SLESSLB_MODE_NOTSUPPORTED	1283	0x503	Sessionless vserver must have MAC or IPTUNNEL mode set

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_SLESSLB_SVC_USIPNOTSET	1284	0x504	Service bound to a sessionless vserver must have UseSourceIP mode enabled
NSERR_WILDCARDVIP_LBMETHOD_INVAL	1286	0x506	Invalid LB method for a wildcard vserver
NSERR_WILDCARDVIP_PERSIST_INVAL	1287	0x507	Invalid persistence policy for a wildcard vserver
NSERR_LB_SO_THRESHOLD	1288	0x508	Spill-over threshold should be a non-zero value
NSERR_CONNFAILOVER_USIP	1289	0x509	Service must have Use Source IP option set in order to be bound to a connection failover enabled virtual server
NSERR_CONNFAILOVER_SERVICE	1290	0x50a	Connection failover can only be enabled on a virtual server of service type ANY
NSERR_LB_SO_DYNAMICCON_THRESHOLD	1291	0x50B	Spill-over threshold cannot be set for dynamic connection spill-over method
NSERR_LB_SO_ADDRVIP	1292	0x50C	DYNAMICCONNECTION spill-over cannot be set on a non-LB vserver

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_CONNFAILOVER_NOTFOR_SLESS	1293	0x50d	Connection Failover is not supported for sessionless lb vserver\n
NSERR_NEWSVC_PERCENT_CAPPED	1294	0x50e	Percentage value of requests capped at 100
NSERR_SIP_NOCALLID	1296	0x510	Missing Call-ID header field
NSERR_SIP_NOVIA	1297	0x511	Missing Via header field
NSERR_SIP_NOCSEQ	1298	0x512	Missing CSeq header field
NSERR_SIP_NOTO	1299	0x513	Missing To header field
NSERR_SIP_NOFROM	1300	0x514	Missing From header field
NSERR_SIP_NOMAX_FORWARDS	1301	0x515	Missing Max-Forwards header field
NSERR_SIP_SERVICE_UNAVAILABLE	1302	0x516	Service unavailable
NSERR_SVC_NOT_BOUND	1303	0x517	Service not bound to Vserver
NSERR_SVCTYPE_MISMATCH	1304	0x518	Service type mismatch between the vserver and service

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_CH_CON_NOT_ALLOWED	1305	0x519	CONNECTION header cannot be set
NSERR_LBPROFILE_DBS	3572	0xdf4	DBSLB setting of LB profile cannot be changed with vservers associated with it
NSERR_LBPROFILE_EXIST	3573	0xdf5	LB profile already exists
NSERR_LBPROFILE_NOENT	3574	0xdf6	LB profile doesn't exist
NSERR_LBPROFILE_NOMEM	3575	0xdf7	Cannot allocate memory for LB profile
NSERR_LBPROFILE_VSERVERSET	3576	0xdf8	Cannot set vserver params which is associated with LB profile
NSERR_CH_INCOMPLETE_HDR	1312	0x520	Custom Header string should end with CRLF
NSERR_SPILLOVERDISABLED	1313	0x521	No spillover on the vserver due to max client setting '0' on a bound service
NSERR_MAXTIMEEXCEEDED	1314	0x522	Maximum time value for interval or responsetimeout or downtime is exceeded, rounding to maximum

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_SCINVALPROTO	1315	0x523	Cannot bind SC policy to non-HTTP service or vserver
NSERR_ROOTREC	1316	0x524	Atleast one nameserver record should exist for the root domain
NSERR_ROOT_GLUEREC	1317	0x525	Root domain nameserver address record should have atleast one ip address
NSERR_VIPINSERT_NOT_SUPPORTED	1356	0x54c	Vserver IP and port header insertion option not supported on this vserver.
NSERR_VSVR_ALRDY_BOUND	1318	0x526	This vserver is already bound to a WLM
NSERR_INVALID_WLM_BINDING	1319	0x527	Only LB vservers are allowed to bound to WLM
NSERR_VSVR_NOT_BOUND	1320	0x528	Vserver not bound to WLM
NSERR_WLM_EXISTS	1321	0x529	WLM already configured on this IP, port
NSERR_INVALID_TIMEOUT	1322	0x52a	Invalid persistence timeout: default timeout assigned

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_CONNFAILOVER_TCPB	1324	0x52c	Stateful connection failover cannot be enabled on a vserver that binds services with TCP buffering enabled
NSERR_CONNFAILOVER_TCPB_SVC_BIND	1326	0x52e	Service with TCP buffering enabled cannot be bound to a vserver with stateful connection failover enabled
NSERR_CONNFAILOVER_TCPB_SVC_PARAM	1327	0x52f	TCP buffering cannot be enabled on a service bound to a vserver with stateful connection failover enabled
NSERR_CONNFAILOVER_SERVICE_STATEFULL	1328	0x530	Stateful connection failover cannot be enabled on a vserver of this service type
NSERR_CONNFAILOVER_SSL_SVC_BIND	1329	0x531	SSL TCP service cannot be bound to a TCP vserver with stateful connection failover enabled
NSERR_CONNFAILOVER_SSL_SVC	1331	0x533	Stateful connection failover cannot be enabled on a vserver that binds services of type SSL_TCP
NSERR_INVALID_PERSISTENCE	1332	0x534	Invalid Persistence type

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_RTSPSESSION_INVALID	1333	0x535	Invalid RTSP session entry
NSERR_LB_METHOD_SAMEAS_BACKUP_METHOD	1334	0x536	Backup load balancing method cannot be the same as the primary load balancing method
NSERR_SERVER_EXIST	1335	0x537	Server already exists
NSERR_LB_SO_HEALTH	1336	0x538	HEALTH spill-over cannot be set on a non-LB vserver
NSERR_REQ_RULE_MISSING	1337	0x539	Request Rule is required, when Response rule is specified.
NSERR_CONNFAILOVER_BINDLO	1338	0x53a	Loopback service cannot be bound to vserver with connection failover enabled \n
NSERR_CONNFAILOVER_SETWITHLO	1339	0x53b	Connection Failover cannot be set to STATEFUL/ STATELESS on vserver with bound loopback service\n
NSERR_REDIRECT_URL_NOT_APPLICABLE	1340	0x53c	Redirect URL cannot be configured on this vserver.

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_CONNFAILOVER_NOT_SUPPORTED	1342	0x53e	Connection Failover is not supported for pattern based vservers
NSERR_NOBIND_ONPUSH	1343	0x53f	Bindings not allowed on push vserver
NSERR_PUSH_VSVR	1344	0x540	Option cannot be set on push vserver
NSERR_ONLY_HTTPSSL	1345	0x541	Option can only be set on http/ ssl vserver
NSERR_PUSH_BIND_EXISTS	1346	0x542	A push vserver is already bound. Unbind before binding new vserver
NSERR_SET_PUSHVS_ONLY	1347	0x543	Push vserver should be of type push or ssl_push only
NSERR_SLESS_NO_SUPPORT	1348	0x544	Not supported for sessionless vservers
NSERR_LISTEN_POLICY_BIND	1351	0X547	Error in binding listen policy to vserver(normal vserver is already present)
NSERR_NO_LISTEN_POLICY_FOR_DUMMYVS	1352	0x548	Cannot bind listen policy to dummy vservers
NSERR_LISTEN_POLICY_BIND_PRESENT	1353	0X549	Error in binding listen policy to vserver(vserver with

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
			new priority is already present)
NSERR_NO_LISTEN_PRI	1354	0X54a	Error in binding listen priority to normal vserver
NSERR_NORMAL_VS_NONE_LISTENPOL	1355	0x54b	The vserver already has None Listen Policy\n
NSERR_NO_LISPRI_FOR_NONE_LISPOL	1357	0x54d	None listenpolicy does not have listen priority\n
NSERR_INVALID_POLICY_STRING	1358	0x54e	Invalid listenpolicy entered\n
NSERR_NODATALENOFFFORVS	1359	0x54f	Dataoffset and datalength are not required for this vserver\n
NSERR_LBGRPPERSISWITHRDP	1285	0x505	Persistency is not applicable for RDP vserver or LB group which has RDP vserver part of it
NSERR_CS_SOTHRESHOLD	1370	0x55a	Spillover threshold must be given with spillover method in Content Switching vserver
NSERR_INVALID_INSERTVSERVERIPPORT	1392	0x570	V6TOV4MAPPING is not applicable to ipv4 vserver

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_LB_SERVER_NOTEXIST	1388	0x56c	The Target LB Vserver does not exist
NSERR_BOUNDTO_CSACT	1371	0x55b	The Vserver referred by Content Switching action cannot be removed
NSERR_BOUNDTO_CSPOLICY	1372	0x55c	The Content Switching Action bound to Content Switching Policy cannot be removed
NSERR_INVALID_MULTIPLEBIND	1373	0x55d	Multiple Bind not supported for Content Switching Advanced policies without action
NSERR_CSPOLICY_HASACTION	1374	0x55e	LB vserver/ gotoPriorityExpression/invoke not allowed during bind when content switching policy already has an action.
NSERR_CS_NOTSUPPORT_LB	1375	0x55f	The Protocol of given LB vserver is not supported by Content Switching action
NSERR_ACTION_NOTNOOP_CS	1386	0x56a	Do not provide gotoPriorityExpression/invoke because policy has action

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_CSPOLICY_NOACTION	1387	0x56b	Either LB vserver or GotoPriorityExpression or Invoke must be provided while binding a Content Switching policy without action.
NSERR_POLICY_USED_FOR_INVOKE	1390	0x56e	Do not give target LB because the policy has been bound to multiple entities
NSERR_SPECIFY_BACKUP_NODE	1393	0x571	Please specify the backup node.
NSERR_SAME_NODES	1394	0x572	Owner and backup nodes need to different.
NSERR_TCPKA_IDLETIME_TOO_LOW	1396	0x574	Connection idle time cannot be lower than keep-alive probe interval
NSERR_OWNER_NODE_NOT_IN_CLUSTER	1397	0x575	Owner node is not in the cluster config or is NOT ACTIVE
NSERR_BACKUP_NODE_NOT_IN_CLUSTER	1398	0x576	Backup node is not in the cluster config or is NOT ACTIVE
NSERR_SPOTTED_VSERVER_NOT_SUPPORTED_IN_STANDALONE	1399	0x577	Spotted vserver configuration not supported in standalone or HA deployment

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_SPOTTED_CONFIG_NO_MATCH	1400	0x578	Spotted config of the backup vserver does not match the vserver
NSERR_OPTION_NOT_SUPPORTED	1401	0x579	Skip persistency is supported only for ANY and UDP service types
NSERR_OPTION_NOT_SUPPORTED_IP	1402	0x57a	BYPASS is not supported for IP based vservers
NSERR_OWNER_NODE_NOT_SET	1403	0x57b	Owner node should be specified for cluster
NSERR_INVALID_RENAME	1404	0x57c	Rename is supported only for Advanced policies
NSERR_INVAL_LOCAL_NAMSVR_TYPE	1405	0x57d	Only UDP based local nameservers are allowed
NSERR_INVALID_TFTPORT	1406	0x57e	Invalid port for tftp vserver
NSERR_NO_RENAME	1407	0x57f	No Rename Supported
NSERR_USE_BIND CR_CMD	88	0x58	Use Bind CR command to bind CR Vserver instead of Bind CS
NSERR_NOENT_AS_PROFILE	1408	0x580	No such Autoscale profile

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_LBREFFERED_IN_CSBINDING	1409	0x581	Cannot remove LB Vserver which is referred to in CS/CR policy bindings
NSERR_DEFAULTLB_NOT_BOUND	1410	0x582	default LB mentioned is not bound
NSERR_NG_BIND_ENTITY	1411	0x583	Error binding the node group to an entity
NSERR_ENTITY_BOUND_TO_ANOTHER_NG	1412	0x584	The specified entity is already bound to a different node group
NSERR_ENTITY_ALREADY_BOUND	1413	0x585	The specified entity is already bound to this node group
NSERR_ENTITY_NOT_BOUND_TO_NG	1414	0x586	The specified entity is not bound to any node group
NSERR_NG_NOT_FOUND	1415	0x587	Nodegroup is not found
NSERR_NG_HAS_BINDINGS	1416	0x588	Nodegroup cannot be deleted, it has entities bound to it
NSERR_VSERVER_CANNOT_BIND	1417	0x589	Vserver cannot bind to the nodegroup
NSERR_VSERVER_CANNOT_UNBIND	1418	0x58a	Vserver cannot unbind to the nodegroup
NSERR_NG_CANNOT_BE_STRICT	1419	0x58b	Nodegroup cannot be made strict as there are no nodes

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
			bound to it, but entities are bound
NSERR_NG_STRICT_AND_ZERODEPTH	1420	0x58c	Cannot bind an entity to a strict nodegroup with no nodes bound to it
NSERR_UNBINDING_LAST_NODE_FROM_STRICT_NG	1421	0x58d	Cannot unbind the last node from a strict nodegroup with entities bound to it
NSERR_NG_ALREADY_ADDED	1422	0x58e	Nodegroup is already added
NSERR_NG_ENTITY_NOMEM	1423	0x58f	No memory to establish entity to nodegroup association
NSERR_NG_MAX_CONFIGURED	1424	0x590	Cannot add nodegroup; maximum number of nodegroups already added
NSERR_INVAL_CS_ACTION	1425	0x591	Action given is not a CS action
NSERR_SET_CSACTION_DISALLOWED	1426	0x592	Set disallowed for CS action from Target LB/ targetVserver to Target Expression and vice versa
NSERR_RETAIN_VLAN	1427	0x593	macmoderetainvlan applicable only for wildcard(IP and port) macmode vserver.

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
			Disable macmoderetainvlan attribute to change the mode of vserver
NSERR_BIND_BDGGROUP_SYNCVLAN	1428	0x594	Sync vlan cannot be bound to bridgegroup
NSERR_DEL_SYNCVLAN	1429	0x595	Sync vlan cannot be deleted
NSERR_LESSTHAN_PPE	1438	0x59e	Max/Min Reusepool connections should be greater than or equal to running Packet Engines.
NSERR_MCLIMITS	1295	0x50f	Dummy error to avoid issues when upgrade done from 9.3.
NSERR_SIP_BAD_REQUEST	1431	0x597	Invalid SIP request.
NSERR_SIP_NO_CONTENT_LEN	1432	0x598	No content length present.
NSERR_SIP_RET_MAX_INCOM_LEN	1433	0x599	SIP InComp max limit reached.
NSERR_SIP_RET_RETRY	1434	0x59a	SIP packet retry.
NSERR_SIP_RET_NO_MEM	1435	0x59b	SIP no memory available.
NSERR_SIP_RET_HEADER_NOT_COMPLETE	1436	0x59c	Incomplete SIP headers.

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_SIP_RET_FAILURE	1437	0x59d	SIP operation failed.
NSERR_CS_GSLB_DEFAULT	1439	0x59f	Default vserver type mismatch
NSERR_CS_GSLB_DNSRT_MISMATCH	1306	0x51a	DNSrecordType of CS GSLB vserver and Target Vserver should be same.
NSERR_CS_GSLB_INVALID_TARGET	1307	0x51b	CS Vserver of type GSLB can only have GSLB vserver as Target.
NSERR_CS_GSLB_POLICY_NO_ACTION	1308	0x51c	CS Policy has no action or CS action doesn't have targetVserver
NSERR_GSLB_SVC_ALREADY_BOUND_TO_CS	1309	0x51d	GSLB service bound to targetVserver is already bound to CS vserver
NSERR_CS_POLICY_NO_RULE	1310	0x51e	Binding CS policy to CS GSLB vserver requires rule
NSERR_VIP_BACKUP_ISCSGSLB	1311	0x51f	CS GSLB vserver cannot be backup of a non- CS GSLB vserver
NSERR_VSR_BOUND	1325	0x52d	Service/servicegroup is bound to one or more vserver. Please unbind and retry the operation. Also check

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
			'allowBoundSvcRemoval' option in lb parameter to change this behaviour.
NSERR_SG_AUTOSCALE_REQ_SRV	1504	0x5e0	Autoscale DNS must be enabled on servicegroup for binding server of SRV querytype
NSERR_SG_PORT_REQ	1505	0x5e1	Port is not specified
NSERR_SRV_PORT_NREQ	1506	0x5e2	Port should not be specified for DBS server of SRV querytype
NSERR_DBS_SPECIFIC_PARAMS	1507	0x5e3	This parameter can only be used for DBS type servers
NSERR_LW_CPX	1687	0x697	Operation not permitted
NSERR_DESIREDSTATE_FAILED	1442	0x5a2	Failed to bind some servicegroup members
NSERR_UNBIND_TROFS_ITEM	1443	0x5a3	Cannot perform unbind operation on graceful unbind service group members
NSERR_SGRP_MEMBER	1690	0x69a	Cannot set/unset graceful unbind/ graceful delay parameters on

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
			service group members
NSERR_NS_VARIABLE_INVALID_INPUT	1692	0x69c	NS Variable should start with $ and Name of NS Variable cannot be greater than 127 (excluding the '$')
NSERR_NS_VARIABLE_MISCONFIGURATION	1693	0x69d	Variable is not configured as expected. Variable should be configured with scope transaction, type TEXT with value-max-size of at most 255
NSERR_COOKIE_ATTR_INVALID_CHAR	1730	0x6c2	Configured literalADCCookieAttribute parameter contains invalid character
NSERR_LITERAL_COMPUTED_MUTEX	1731	0x6c3	Either literalADCCookieAttribute or computedADCCookieAttribute is already set

LB2 ERRORS

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_ADDRPRESENT	1376	0x560	Address(s) is invalid or already present in

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
			this action, will be discarded.
NSERR_PERSISTENCE_PERSISTAVP_NOTDEFINED	1377	0x561	Persist Avp Number Must be defined For diameter Persistency
NSERR_MAX_DIAMETER_AVP_EXCEEDED	1378	0x562	Maximum number of diameter Persist Avp Codes exceeded
NSERR_AUTOSCALE_MIN_GT_MAX	1379	0x563	Minimum Autoscale member count exceeds the maximum value
NSERR_MEMBERPORT_REQD	1380	0x564	Member Port option has to be specified when autoScale option POLICY is chosen
NSERR_COOKIEINSERT_NOTSET	1381	0x565	Persistence type is not COOKIEINSERT.
NSERR_LB_POLICY_NSB_FREED	2286	0x8ee	LB policy evaluation freed the NSB
NSERR_LB_ACT_MUSTBE_NOLBACTION	2287	0x8ef	Non-terminating LB policy must have NOLBACTION/ ASSIGNMENT action

LSN ERRORS

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_LSN_NOPOOL	3960	0xf78	No such pool
NSERR_LSN_NOTRANSPRFL	3961	0xf79	No such transportprofile
NSERR_LSN_NOAPPSPRFL	3866	0xf1a	No such applicationprofile
NSERR_LSN_POOLNOTBOUND	4052	0xfd4	Pool not bound to group
NSERR_LSN_PRFLNOTBOUND	4053	0xfd5	Profile not bound to group
NSERR_LSN_NOTREADY	4054	0xfd6	LSN not initialized. Please check memory allocated to LSN.
NSERR_LSN_MAXBINDINGS	4055	0xfd7	Maximum bindings allowed exceeded
NSERR_LSN_ACL_DETERMINISTICNAT	4056	0xfd8	Client with ACLs not allowed for deterministic nat
NSERR_LSN_ACLTYPE	4057	0xfd9	ACL with action other than ALLOW or establishedflag set
NSERR_LSN_ACLINUSE	4058	0xfda	ACL already bound to an LSN/RNAT rule
NSERR_64LIB_MEM_NOTSUFFICIENT	4059	0xfdb	Active memory less than minimum required for LSN and Subscriber Session Store

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_LSN_NOBINDING	4060	0xfdc	No such binding
NSERR_LSN_NONETWORK	4061	0xfdd	No such network
NSERR_LSN_CLIENTGROUP	4062	0xfde	Please remove client's group first
NSERR_LSN_NOCLIENT	4063	0xfdf	No such client
NSERR_LSN_NOGLBLLOG	4072	0xfe8	Logging is disabled at Global level
NSERR_LSN_CLIENTINUSE	4080	0xff0	Client is already present in a group
NSERR_LSN_PORTBLOCKSIZE	4081	0xff1	Portblocksize should be multiple of 256
NSERR_LSN_WRONG_PORTBLOCKSIZE	855	0x357	Portblocksize should not exceed 64512
NSERR_LSN_BINDINGEXIST	4082	0xff2	Binding already exists
NSERR_LSN_POOLGROUPTYPE	4083	0xff3	Both pool and group should be of same nat type
NSERR_LSN_POOLREUSE_DETERMINISTICNAT	4084	0xff4	Pool can be bound to only one group for determinstic nat
NSERR_LSN_PORT_APPSPROFEXIST	4085	0xff5	Profile already exists for one or more ports in this/bound group(s)

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_LSN_TCPONLY	4086	0xff6	Allowed only for TCP profile
NSERR_LSN_MAPPINGFILTERINGTYPE	4087	0xff7	Filtering should be more or equally strict as mapping
NSERR_LSN_ICMPAPPSPROF_MAPPINGFILTERINGPORT	4088	0xff8	Port dependent Filtering or Mapping not allowed for ICMP
NSERR_LSN_ICMPAPPSPROF_PORT	4089	0xff9	Port bindings not allowed for ICMP applicationprofile
NSERR_LSN_STATIC_NOGROUP	4090	0xffa	Client ip not part of any active lsn group
NSERR_LSN_STATIC_INVPOOL	4091	0xffb	No natip available or natip given is invalid
NSERR_LSN_FINTIMGTSESSTIM	4092	0xffc	Finrsttimeout should not be more than session timeout
NSERR_LSN_SETPORTBLOCK_DETERMINISTICNAT	4093	0xffd	Port block size cannot be modified for deterministic nat
NSERR_LSN_DETERMINISTICNAT_SUBSCR_LIMIT	4094	0xffe	Maximum allowed subscribers for deterministic nat group exceeded
NSERR_64LIB_MEM_INCOMPLETE	3943	0xf67	Active memory could be different from configured memory limit, Please check 'show

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
			extendedmemoryparam'
NSERR_64LIB_MEM_EXCEEDSMAX	3944	0xf68	Configured memory cannot exceed maximum limit, Configured memory is set to maximum available limit'
NSERR_64LIB_MEM_SIZE2M	3945	0xf69	Configured memory should be in multiples of 2MB
NSERR_LSN_IPINSERT	3957	0xf75	LSN IP addition failed
NSERR_LSN_ICMP_TIMEOUT_EXCEEDED	3958	0xf76	Maximum value of ICMP session timeout is 240 seconds
NSERR_LSN_TCP_UDP_TIMEOUT_EXCEEDED	3867	0xf1b	Maximum value of TCP/UDP session timeout is 600 seconds
NSERR_LSN_APPSPROF_PORTZERO	4073	0xfe9	Cannot bind/unbind port 0 to Application Profile
NSERR_LSN_MEM_DECR	3995	0xf9b	Active memory cannot be decreased without reboot
NSERR_LSN_NOSIPALGPRFL	3547	0xddb	No such sipalgprofile
NSERR_LSN_REM_APPPROFILE_ALGPROFILE_BOUND	3548	0xddc	Can not remove Appfprofile, SIP ALG profile and RTSP

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
			ALG Profile should be unbound from the groups bound to the Appprofile
NSERR_LSN_UNBIND_APPPROFILE_ALGPROFILE_BOUND	3549	0xddd	Can not unbind to the Appprofile, SIP ALG profile and RTSP ALG Profile should be unbound from the groups bound to the Appprofile
NSERR_LSN_NORTSPALGPRFL	4074	0xfea	No such rtspalgprofile
NSERR_LSN_SIPALGPROF_PORTZERO	4075	0xfeb	Cannot add port 0 to SIP ALG Profile
NSERR_LSN_RTSPALGPROF_PORTZERO	4076	0xfec	Cannot add port 0 to RTSP ALG Profile
NSERR_LSN_IP6PROF_DSLITE	4077	0xfed	With DS-Lite add only Network6
NSERR_LSN_IP6PROF_NAT64	4078	0xfee	With NAT64 add only IP6Prefix
NSERR_LSN_NETWORK6_EXISTS	3546	0xdda	network 6 based LSN client already exists for this network 6 address(Duplicate config)
NSERR_LSN_CLIENTNETWORK_INCORRECT_BINDING	3551	0xddf	Both Client and Network type MUST be of the same type,

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
			IPv4, IPv6 or DS-Lite Deterministic
NSERR_LSN_CLIENTGROUPTYPE	3553	0xde1	Both client and group should be of same type
NSERR_LSN_DSLITEPREFIXLEN	3554	0xde2	Network6 MUST have a prefix length 128 for a DS-Lite DETERMINISTIC type client or client associated with STATIC mapping
NSERR_LSN_NOIP6PROFILE	3555	0xde3	No such IP6 profile
NSERR_LSN_IP6GROUP	4079	0xfef	Please remove associated group first
NSERR_LSN_DSLITE_INVALIDIP6	3556	0xde4	With DS-Lite add only SNIP6.
NSERR_LSN_DSLITE_SNIP6_REQD	3557	0xde5	DS-Lite needs SNIP6 in relevent TDs. If not already present, add SNIP6 relevent to all tds belonging to an LSN group
NSERR_LSN_DUP_IP6PROFILE	3552	0xde0	Either IPv6 address or NAT Prefix already been used
NSERR_LSN_SIPALG_CANNOT_BIND	3882	0xf2a	Cannot bind SIPALG profile to the group, either the group is not in full cone mode

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
			or IP Pool pair is not enabled
NSERR_LSN_RTSPALG_CANNOT_BIND	3883	0xf2b	Cannot bind RTSP profile to the group, either the group is not in full cone mode or IP Pool pair is not enabled
NSERR_LSN_SIPALG_TRANSPORT_PROTOCOL_BINDINGEXIST	3884	0xf2c	Can not bind more than one SIPALG profile of same transport protocol to the lsn group
NSERR_LSN_RTSPALG_TRANSPORT_PROTOCOL_BINDINGEXIST	3885	0xf2d	Can not bind more than one RTSPALG profile of same transport protocol to the lsn group
NSERR_LSN_CANNOT_UNBIND_APPPROFILE	3886	0xf2e	Can not unbind appprofile unless all SIP ALG Profiles, RTSP ALG Profiles and IPSEC ALG Profile are unbound from all the groups to which appsprofile is bound
NSERR_LSN_RTSPALGPROF_TRANSPORT_SUPPORTED	3887	0xf2f	RTSP ALG profile for only TCP is supported
NSERR_LSN_IPSECALG_CANNOT_BIND	3520	0xdc0	Cannot bind IPSECALG profile to the group, IP Pool pair is not enabled

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_LSN_SIPALGPROF_PORT_NOT_ADDED	3353	0xd19	Atleast sipsrcportrange or sipdstportrange should be added with positive portrange
NSERR_LSN_GRP_SESS_LIMIT	852	0x354	Group session limit must be greater than the number of Packet Engines
NSERR_LSN_DETER_POOL	3903	0xf3f	Cannot enable portblock allocation on deterministic pool
NSERR_LSN_SIP_RTSP_ALG_MAPPING_FILTERING_IPPOOLING	853	0x355	Can not set appsprofile unless all SIP ALG profiles and all RTSP ALG profiles are unbound from all the groups to which appsprofile is bound
NSERR_LSN_PORTBLOCKSIZE_NOTALLOWED	856	0x358	Portblock size should not be changed to zero from nonzero and to nonzero from zero
NSERR_LSN_POOLGROUP_PORTBLOCK_MISMATCH	857	0x359	Pool's portblock allocation and group's portblocksize fields are not compatible
NSERR_LSN_GRPID_PERM	3818	0xeea	GroupID should not be explicitly specified

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_LSN_INVALID_DSLITE_PREFIX_LEN	3819	0xeeb	Invalid Ipv6 Prefix length for dslite client ipv6 network(only /128 prefix is allowed)
NSERR_LSN_NOLOGPRFL	3384	0xd38	No such log profile
NSERR_LSN_NOHTTPHDRLOGPRFL	3392	0xd40	No such HTTP header log profile
NSERR_LSN_DOHASYNC	3396	0xd44	Force HA Sync should be given to sync Primary's pre-flush operation LSN sessions
NSERR_LSN_STATICWILD_INV_PORT	3397	0xd45	invalid port for static nat wild card port config, subscr port and nat port must be *
NSERR_LSN_STATICWILD_INV_NATIP	3398	0xd46	NAT ip must be given for static nat wildcard port config
NSERR_LSN_STATICWILD_INV_DSTIP	3399	0xd47	Dest ip must not be given for static nat wildcard port config
NSERR_LSN_STATICWILD_INV_WILDPORT	3400	0xd48	wild card port(* or 65535) is valid only for transport protocol type ALL(i.e. only static nat wild card port config)

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_LSN_STATICWILD_NATIP_INUSE	3401	0xd49	NAT ip is already in use for static nat wildcard port config.
NSERR_LSN_STATICWILD_NATIP_NO_FREE_PORTS	3402	0xd4a	NAT ip is not valid or not all ports on NAT ip are free, select different natip which has all ports free.
NSERR_LSN_NAT64_MAP_INS_FAIL	3406	0xd4e	Operation on nat64 prefix failed due to low system memory
NSERR_LSN_DSLITE_NO_FTP_CM	3577	0xdf9	FTP connection mirroring in LSN is not supported with DS-Lite nattype

MAP DOMAIN ERRORS

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_MAP_IPV6_PREFIX_INVALID	3529	0xdc9	MAP IPv6 Prefix is invalid, it must be global
NSERR_MAP_IPV6_PREFIX_REQ	3530	0xdca	MAP IPv6 Prefix is required
NSERR_MAP_PSID_INVALID	3531	0xdcb	MAP BMR Port Set ID is invalid
NSERR_MAP_PSID_OFFSET_INVALID	3532	0xdcc	MAP BMR Port Set ID offset is invalid
NSERR_MAP_IPV4_NW_REQ	3533	0xdcd	MAP BMR rule ipv4 network and netmask

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_MAP_BMR_NW_MISSMATCH	3534	0xdce	MAP BMR rule and ipv4 network mismatch
NSERR_MAP_BMR_PSID_LEN_INVALID	3535	0xdcf	MAP BMR rule sharing ration is invalid it must be 1 to 16
NSERR_MAP_BMR_EABIT_LEN_INVALID	3543	0xdd7	MAP BMR rule EABIT length invalid
NSERR_MAP_NSB_CONSUMED	3544	0xdd8	NSB is consumed by MAP-T, error return to source or packet forwarded
NSERR_MAP_NO_CONFIG	3545	0xdd9	NO MAP T config, continue with other config

NAT64 ERRORS

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_NAT64_ACL_EXISTS	3959	0xf77	ACL is bound to another NAT64 rule

NET ERRORS

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_ACL_TIMED_OUT	977	0x3d1	ACL timed out

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_MSR_ADVT_NULL_RT	978	0x3d2	Cannot monitor or advertise NULL route
NSERR_DEF_RT_UNSET	979	0x3d3	Unset operation on default route not allowed
NSERR_ACTIVE_PERM_DIR_NULL_RT	981	0x3d5	Unset operation on active or permanent or direct or null routes not allowed
NSERR_DHCP_RT	982	0x3d6	Unset operation on DHCP route not allowed
NSERR_LB_RT	983	0x3d7	Unset operation on LB route not allowed
NSERR_MSR_STATIC_RT	984	0x3d8	Cannot set MSR on a non-static route
NSERR_ADV_DEF_RT	985	0x3d9	Advertise on default route not allowed
NSERR_VLAN_RT	986	0x3da	Cannot delete this route. Network is bound to VLAN
NSERR_PERM_RT	987	0x3db	A permanent route cannot be deleted
NSERR_NOENTRY_RT	988	0x3dc	Entry not found in the routing table
NSERR_DIR_RT	989	0x3dd	Cannot add a direct route
NSERR_LOOP_RT	990	0x3de	Cannot add a route in loopback network

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_GW_NWID_BROADADDR	991	0x3df	Gateway cannot be network id or broadcast address
NSERR_MON_ADV_NULL_RT	992	0x3e0	Cannot set MSR or advertise on null gateway
NSERR_HA_PEER_IP	994	0x3e2	Cannot add IP address. This is peer's NSIP
NSERR_NON_LOCAL_IP	995	0x3e3	IP address is already configured on a node in the cluster
NSERR_ADD_NSIP	996	0x3e4	Adding NSIP not allowed
NSERR_VRID_VIP_ONLY	997	0x3e5	VRID can be set only on VIP
NSERR_ARP_ICMP_SNIP_NSIP	998	0x3e6	ARP and ICMP cannot be disabled on SNIP/NSIP/MIP/CLIP
NSERR_IPADDR_DISABLE	999	0x3e7	IP address state of SNIP/NSIP/CLIP cannot be disabled
NSERR_NODE_NOEXIST	1000	0x3e8	Cluster node does not exist
NSERR_CLIP_SPOTTED_IP	1001	0x3e9	CLIP should be striped
NSERR_IP_MGMTACCESS	1002	0x3ea	Management Access cannot be enabled on this IP address

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_IPTUN_MULTICAST	1003	0x3eb	Vlan on which to send the packet needs to be specified for multicast remote endpoints
NSERR_IPTUNNEL_INVALIDNETMASK	1004	0x3ec	IP tunnel netmask should be 255.255.255.255
NSERR_IPTUNNEL_VLAN	1005	0x3ed	Vlan can be specified only for multicast remote endpoints
NSERR_IPTUN_INV_LIP	1006	0x3ee	Invalid local IP address. Either the local IP address is not configured or local IP address has to be one among SNIP|VIP|MIP
NSERR_VXLAN_LIP_NOT_SNIP	1007	0x3ef	Invalid local IP address. For VXLAN local IP address has to be SNIP
NSERR_INVALID_IPTUNNEL_NAME	1008	0x3f0	Invalid IPTunnel name
NSERR_IPTUNNEL_PREFXLEN_GT_128	1009	0x3f1	IP tunnel prefix length should not be more than 128
NSERR_TUN_PBR_DEP	1010	0x3f2	Cannot remove tunnel. A PBR is depending on this tunnel

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_TUN_NOEXIST	1011	0x3f3	Tunnel does not exist
NSERR_INV_DROPFRAGCPUTHRESH	1012	0x3f4	Invalid dropFragCpuThreshold parameter. Should >=1 and <=100
NSERR_SRCIP_NOEXIST	1013	0x3f5	SrcIP does not exist
NSERR_TUN_ON_DEF_ROUTE	1014	0x3f6	Cannot add tunnel on default route
NSERR_VLAN_NOT_SNIP_MIP_VIP	1015	0x3f7	IP address has to be either SNIP, MIP or VIP
NSERR_ACL_PROTO_TCP	1016	0x3f8	Protocol should be TCP for ESTABLISHED flag to be set
NSERR_HA_VERSION_MISMATCH	1017	0x3f9	HA version mismatch between primary and secondary
NSERR_HA_SYNC_VLAN	1018	0x3fa	Syncvlan should be L2 VLAN. No IP address should be bound to this VLAN
NSERR_LOOP_FIS	1019	0x3fb	Loopback interface cannot be bound to Failover Interface Set (FIS)

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_VLAN_LOOP	1020	0x3fc	Loopback interface cannot be unbound from default VLAN
NSERR_VLAN_TAGG_INTF_NOSUPP	1021	0x3fd	VLAN tagging is not supported on this platform/interface
NSERR_VLAN_BDG_NOTBOUND	1022	0x3fe	The VLAN is not bound to specified bridgegroup
NSERR_PERMANENT_ARP_ND6_ENTRY	1023	0x3ff	Can't remove permanent ARP/ND6 entry
NSERR_HA_VER_MISMATCH_PROP_SYNC	1447	0x5a7	HA version mismatch. Prop and sync not allowed
NSERR_VXLAN_TUNN_BOUND	1458	0x5b2	Cannot remove IPtunnel. One or more VXLAN is bound to this iptunnel.
NSERR_HOSTRT_UNSET	1489	0x5d1	Unset of OSPFArea and HostRtGw is allowed only for VIP
NSERR_BDGGRP_L3VLAN	2412	0x96c	L3VLAN cannot be bound to a bridgegroup
NSERR_BDGGRP_ROUTING	2505	0x9c9	Routing is enabled on the specified VLAN. Cannot bind this VLAN to the bridgegroup

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_RM_RT_DIR_PERM_DHCP	2506	0x9ca	DIRECT/ PERMANENT/DHCP routes cannot be removed.
NSERR_ADD_IP_STRIPED_EXISTS	2507	0x9cb	Trying to add a striped IP address as a spotted IP.
NSERR_DIS_IP_NOT_USR_DEF	2508	0x9cc	Enabling/Disabling this IP address not allowed as VIP is not user-defined
NSERR_DIS_IP_NOT_VIP	2509	0x9cd	Enabling/Disabling this IP address not allowed as it is not VIP
NSERR_DEL_NSIP	2510	0x9ce	Cannot delete NSIP
NSERR_DEL_DHCP_AQRD	2511	0x9cf	Cannot delete DHCP acquired IP address
NSERR_USR_DEF_NO	2618	0xa3a	Not a user-defined IP address
NSERR_TUNL_DEPENDENCY	2619	0xa3b	Existing tunnel depends on this IP address
NSERR_MGMT_NSIP_CLIP	2620	0xa3c	Management access on NSIP and CLIP should always be enabled
NSERR_INV_ICMP_RESP	2621	0xa3d	Invalid icmpResponse value

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_INV_ARP_RESP	2622	0xa3e	Invalid arpResponse value
NSERR_INTERNAL_ERR_REGN	2623	0xa3f	Internal error while registration of service. Service name in use
NSERR_CANT_SET_IP_DEL_IN_PROG	2540	0x9ec	Delete IP address is in progress.
NSERR_INAT_USE_PROXY	2394	0x95a	Useproxyport cannot be disabled when either of publicIP or private IP is IPV6
NSERR_GSLB_ADNS_CONFGRD	2395	0x95b	GSLB/ADNS/RADIUS is already configured on this IP address
NSERR_NW_ADDR_ZERO	2396	0x95c	Network address cannot be zero
NSERR_NW_ADDR_LOOP	2397	0x95d	Network address cannot be loopback
NSERR_UNABLE_DEFVLAN_INFO	2398	0x95e	Unable to get default VLAN info.
NSERR_HA_INC_SYNC	2399	0x95f	SyncVlan is not supported in HA-INC mode
NSERR_IP_NWADDR	2400	0x960	IPaddress cannot be network address
NSERR_IP_BCASTADDR	2401	0x961	IPaddress cannot be broadcast address

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_ACL_BOUND_LSN	2402	0x962	This ACL is already bound to LSN
NSERR_SUBNET_BOUND_ANTHR_VLAN	2403	0x963	Either the subnet is not directly connected or subnet already bound to another VLAN
NSERR_DEL_ADNS_IP	2406	0x966	Cannot delete this IP address as ADNS is configured on this.
NSERR_DEL_REF_IP	2407	0x967	Cannot delete this IP address as it is used in GSLB/IPSET/ Other entities
NSERR_SNMP_CANNOT_EN_ON_IP	2409	0x969	SNMP cannot be enabled on this IP address
NSERR_CANNOT_EN_ON_IPADDR	2410	0x96a	SNMP/TELNET/FTP/ SSH/GUI/SECURE GUI/RESTRICTED-IP cannot be enabled on this IP address
NSERR_ACL_ESTABLISHED_SET	2414	0x96e	For RNAT/NAT64 ACL established flag cannot be set
NSERR_DEL_RADIUS_IP	2415	0x96f	Cannot delete this IP address as RADIUS is configured on this.
NSERR_CANNOT_EN_ON_IP	2416	0x970	TELNET/FTP/SSH/ GUI/SECURE GUI/ RESTRICTED-IP

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
			cannot be enabled on this IP address
NSERR_BFD_SESSION_CLEAR_INPROGRESS	2418	0x972	BFD session cannot be added now as old session clear is in progress
NSERR_BFD_SESSION_EXISTS_DIFF_FLAGS	2419	0x973	BFD session exists with different flags (SINGLEHOP AND MULTIHOP)
NSERR_CLASS_E	2426	0x97a	Class-E IPv4 and IPv6PT are mutually exclusive configs. Disable one to enable the other
NSERR_TUN_CIPROF_DEP	2427	0x97b	Cannot remove tunnel. A Content Inspection profile is depending on this tunnel
NSERR_FEA_NOT_SUPPORTED	2428	0x97c	Feature not supported on this platform
NSERR_HTTP_SSL_SAME_VALUE	2429	0x97d	HTTP and SSL cannot have same Management Port Value.
NSERR_FEA_NOT_SUPPORTED_LPCPX	2430	0x97e	Feature not supported on CPX without privilege
NSERR_HTTPD_CONF_SAME_VALUE	2431	0x97f	The same HTTPD max clients/max request workers

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
			value cannot be configured
NSERR_HTTPD_CONF_MUTUALLY_EXCLUSIVE	2435	0x983	Both, HTTPD max clients and max request workers value cannot be configured at the same time.
NSERR_HTTPD_CONF_UPDATE_FAILED	408	0x198	Failed to update HTTPD configuration file. Check /var/log/ns.log for details.
NSERR_HA_DE_MISMATCH	409	0x199	Disk Encryption mismatch between HA Nodes.

NETBRIDGE ERRORS

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_TNL_NETBRIDGED	3920	0xf50	Tunnel bound to netbridge
NSERR_TNL_GRE	3921	0xf51	Tunnel protocol is not GRE or GENEVE
NSERR_TNL_RIPMASK	3922	0xf52	Remote IP mask of the tunnel should be 255.255.255.255
NSERR_VLAN_NETBRIDGED	3923	0xf53	Vlan already bound to some netbridge
NSERR_MAX_NETBRIDGE_TUNNEL	3924	0xf54	reached maximum netbridge tunnel bindings

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_TUN_BOUND	3925	0xf55	Tunnel already bound to this netbridge
NSERR_SUBNET_BOUND	3926	0xf56	Subnet already bound to this netbridge
NSERR_TUN_CONF_NETBRIDGE	3927	0xf57	Tunnel is not configured
NSERR_VLAN_CONF_NETBRIDGE	3928	0xf58	Vlan is not configured
NSERR_IP_INVAL_NETBRIDGE	3929	0xf59	IP is not bound to netbridge
NSERR_IPV6_INVAL_NETBRIDGE	3930	0xf5a	IPV6 is not bound to netbridge
NSERR_INV_NETBRIDGE_NAME	3931	0xf5b	Netbridge name should be >=1 and <=32
NSERR_GRE_IPSEC_LIP_NOT_GIVEN	3932	0xf5c	Local ip address has to be given for GRE, IPSEC and broadcast VXLAN tunnels
NSERR_NETBRIDGE_TUNNELBOUNDTOPBR	3933	0xf5d	Tunnel is a nexthop for PBR
NSERR_NETBRIDGE_UNSUPPORTEDTUNNELPAYLOAD	3934	0xf5e	GRE Payload should be ETHERNET or ETHERNETwithDOT1Q

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_NETBRIDGE_ONEVLAN_ETHERNET	3935	0xf5f	Only one VLAN can be bound when GRE carries plain ETHERNET
NSERR_NETBRIDGE_TUNNELPAYLOAD_DIFFERENT	851	0x353	All bound tunnels should have same GRE payload

NETPROFILE ERRORS

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_IPSET_REF	3952	0xf70	IP set must be unbound from netprofile before it can be removed
NSERR_NETPROFILE_REF	3953	0xf71	Netprofile must be unbound before it can be removed
NSERR_IPSET_BOUND	3954	0xf72	IP set is already bound to the network profile
NSERR_NO_SUCH_IPSET	3955	0xf73	IP set does not exist
NSERR_NO_SUCH_NETPROF	3956	0xf74	Netprofile does not exist
NSERR_OVERLAPPING_PORTRANGE	3558	0xde6	This range is overlapping the existing portrange.
NSERR_NO_SUCH_PORTRANGE	3559	0xde7	Port range does not exist

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_NO_SUCH_NATRULE	3560	0xde8	natRule does not exist
NSERR_NATRULE_EXIST	3561	0xde9	natrule already exists
NSERR_IP_VSERVER_IPSET_FREE_ERROR	3562	0xdea	Freeing Listening services failed. Please check failure counters

NITRO ERRORS

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_NITRO_INVALID_OBJECTNAME	1232	0x4d0	Invalid object name
NSERR_NITRO_INVALID_JSON_INPUT	1233	0x4d1	Invalid JSON input
NSERR_NITRO_INVALID_JSON_DATATYPE	1234	0x4d2	Invalid JSON data type
NSERR_NITRO_INVALID_XML_INPUT	1235	0x4d3	Invalid XML input
NSERR_NITRO_INVALID_DATATYPE	1236	0x4d4	Invalid NITRO data type
NSERR_NITRO_INVALID_METHOD	1237	0x4d5	Invalid method name. It should be either post, put, get, stat or delete
NSERR_NITRO_PARSE_ERROR	1238	0x4d6	NITRO parse error

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_NITRO_CMDEXEC_FAILED	1239	0x4d7	NITRO command Execution failed
NSERR_NITRO_INVALID_ACTION	1240	0x4d8	Invalid nitro action or operation
NSERR_NITRO_ROLLBACK_FAILED	1241	0x4d9	Rollback failed. Manually correct the configuration
NSERR_NITRO_ROLLBACK_NOT_SUPPORTED	1242	0x4da	Rollback not supported for this action
NSERR_NITRO_BULK_FAILED	1243	0x4db	Bulk operation failed
NSERR_NITRO_BASIC_AUTH_DISABLED	1244	0x4dc	Authentication Failed: Use of Basic Authentication is Disabled.
NSERR_NITRO_TECHSUPPORT_ARCHIVE_CREATION_FAILED	1246	0x4de	Creation of techsupport collector archive failed.
NSERR_NITRO_TECHSUPPORT_ARCHIVE_UPLOAD_FAILED	1247	0x4df	Failed to upload the techsupport collector archive.
NSERR_NSAPP_TEMPLATE_EXISTS	1248	0x4e0	Template already exists
NSERR_NSAPP_INVALID_TEMPLATE	1249	0x4e1	Invalid Template
NSERR_NSAPP_DIR_ERROR	1250	0x4e2	Could not open directory

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_NSAPP_FILE_ERROR	1251	0x4e3	Can not open the file
NSERR_NSAPP_INVALID_APP_INPUT	1252	0x4e4	Invalid Application input
NSERR_NSAPP_EXCEEDED_FILELENGTH	1253	0x4e5	File length exceeded 256 characters
NSERR_NSAPP_ENDPOINT_INUSE	1254	0x4e6	Public endpoint in use
NSERR_NSAPP_PROTOCOL_MISMATCH	1255	0x4e7	Protocol mismatch with existing configuration
NSERR_NSAPP_INVALID_VARNAME	1256	0x4e8	Invalid variable name
NSERR_NSAPP_ZIP_FILE	1257	0x4e9	Error in zip format
NSERR_NSAPP_MAXEP_REACHED	1258	0x4ea	Only one endpoint can be configured
NSERR_NSAPP_NOT_EXIST	1259	0x4eb	Application does not exist
NSERR_NSAPP_INVALID_SERVICETYPE	1260	0x4ec	Invalid servicetype - HTTP/HTTPS/SSL are only allowed
NSERR_NSAPP_TEMPLATE_FORMAT_ERROR	1261	0x4ed	Template format error
NSERR_NSAPP_APP_WITHOUT_APPUNITS	1262	0x4ee	Application without appunits can not be exported

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_NSAPP_SERVICRGROUP_EXISTS	1263	0x4ef	Service group with this name already exists
NSERR_NSAPP_VARIABLE_NOT_EXISTS	1264	0x4f0	Variables do not exist in this template file
NSERR_NITRO_CMD_NOTATTEMPTED	1265	0x4f1	command not attempted for configuration
NSERR_NITRO_INVALIDREQ	1266	0x4f2	Invalid nitro request

NNM ERRORS

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_NNM_FAILED	2528	0x9e0	General NNM failure
NSERR_NNM_CONN_CLEANED	2529	0x9e1	NNM connection was cleaned
NSERR_NNM_CONN_FAILED	2530	0x9e2	NNM connection failed
NSERR_NNM_NO_CONN	2531	0x9e3	NNM connection was not found
NSERR_NNM_CONN_DROPPED	2532	0x9e4	NNM connection dropped
NSERR_NNM_EINJECT	2533	0x9e5	NNM error injection

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_NNM_VERSION_UNSUPPORTED	2534	0x9e6	NNM group payload version is unsupported
NSERR_NNM_TIMEOUT_MSG	2535	0x9e7	NNM timeout unable to send message
NSERR_NNM_TIMEOUT_ACK	2536	0x9e8	NNM timeout waiting for ACK
NSERR_NNM_MCAST	2537	0x9e9	NNM multicast/ broadcast failed
NSERR_NNM_PENDING	2538	0x9ea	NNM operation is in a pending state (e.g., ACK held)

NSTRACE ERRORS

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_ALREADY_RUNNING	3984	0xf90	One instance of nstrace is already running.
NSERR_PKTSIZE_SMALL	3985	0xf91	Packet size must be integer number between 60 - 1514. (0 for full packet trace)
NSERR_CANNOT_CLOSE	3986	0xf92	can not stop nstrace.
NSERR_NSTRACE_PERNIC_WARN	2748	0xabc	can not apply perNIC option with this trace format. Started nstrace without perNIC.

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_NSTRACE_INVALID_FILTER	4064	0xfe0	Invalid filter expression.
NSERR_NSTRACE_SENSITIVE_WARN	2539	0x9eb	The command uses option(s) that may capture confidential information, or keys that can be used to decrypt confidential information into a file. These files have to be stored in a secure environment
NSERR_LOW_DISK	2560	0xa00	Critically low disk space. Please clear disk space under /var

PARTITION ERRORS

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_MAX_PARTITION	2752	0xac0	Maximum allowed partition limit reached
NSERR_PARTITION_NAME_EXIST	2753	0xac1	Partition name already exist
NSERR_NO_PARTITION	2755	0xac3	Partition does not exist
NSERR_DEL_PARTITION_BUSY	2756	0xac4	Partition is busy, can't delete
NSERR_DEL_PARTITION_INUSE	2757	0xac5	Partition is in use, can't delete

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_NO_DEL_DFLT_PARTITION	2758	0xac6	Default Partition can't be deleted
NSERR_RM_PARTITION_CONFIRM	2759	0xac7	Are you sure you want to remove partition (Y/N)? [N]:
NSERR_NOT_SUPPORTFORPARTITION	2760	0xac8	This feature is not supported on partition
NSERR_AP_CONFIG_NOT_ALLOWED	2761	0xac9	This configuration option is not supported on non-default partition
NSERR_VLAN_BDGGRP_PARTITION_EXIST	2762	0xaca	VLAN or VXLAN or BridgeGroup bound to a partition can not be deleted.
NSERR_AP_DEFVLAN	2763	0xacb	Default VLAN cannot be bound/unbound to/from a partition.
NSERR_VLAN_BDGGRP_PARTITION	2764	0xacc	The specified VLAN or VXLAN or BridgeGroup is bound to other partition.
NSERR_PQ_ARG_UNSUPPORTED_PARTITION	2765	0xacd	PQ feature is not supported in non-default partition.
NSERR_SC_ARG_UNSUPPORTED_PARTITION	2766	0xace	SC feature is not supported in non-default partition.

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_MAX_PARTITIONS_ZEBOS	2767	0xacf	Maximum allowed partition limit for routing reached
NSERR_AP_SYNCVLAN	2769	0xad1	SYNC VLAN cannot be bound/unbound to/from a partition.
NSERR_AP_VLAN_BDG_EXIST	2770	0xad2	The specified VLAN cannot be bound to a partition because it is bound to a bridge group.
NSERR_AP_SDXMGMTVLAN	2771	0xad3	The SDX management VLAN cannot be bound/ unbound to/from a partition.
NSERR_AP_DEFAULT_PARTITION_CONFIG	2772	0xad4	This configuration is allowed only from the default partition.
NSERR_AP_MEM_DECR	2773	0xad5	Partition's memory limit cannot be reduced less than currently used memory
NSERR_AP_MISMATCH	2774	0xad6	The specified entity is configured in some other partition.
NSERR_AP_PVID_IF_NOT_ALLOWED	2775	0xad7	The specified VLAN cannot be configured as untagged member of interface because it is bound to partition.

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_AP_VLAN_BINDING_NOT_ALLOWED	2776	0xad8	The specified VLAN cannot be bound to a partition because it is configured as untagged member of interface.
NSERR_AP_NOT_SUPPORTFORSHAREDVLAN	2777	0xad9	This feature is not supported on shared vlan.
NSERR_AP_SHAREDVLAN_CONFIG_NOT_ALLOWED_INCLUSTER	2778	0xada	Configuring vlan as shared is not supported on cluster.
NSERR_AP_SHAREDVLAN_BDG	2779	0xadb	Shared vlan cannot be bound/unbound to/from a bridge group.
NSERR_AP_SHAREDVLAN_TD	2780	0xadc	Shared vlan cannot be bound/unbound to/from a Traffic domain.
NSERR_AP_MCAST_PMAC	2781	0xadd	Partition MAC address cannot have multicast bit set.
NSERR_AP_VMAC_EXIST	2782	0xade	Another admin-partition with the same partition MAC address exist.
NSERR_AP_VMAC_BUSY	2783	0xadf	Partition's MAC address can not be unset when shared vlans are bound to it.

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_AP_XS_CONN_FAILED	2784	0xae0	Unable to communicate with the XenStore.
NSERR_AP_XS_NO_VMAC	2785	0xae1	No partition MAC address is configured for the VPX on SDX.
NSERR_AP_XS_VMAC_NOTEXIST	2786	0xae2	The specified partition MAC address is not configured for the VPX on SDX.
NSERR_AP_XS_VMAC_EXHAUSTED	2787	0xae3	All partition MAC addresses configured for the VPX on SDX are in use.
NSERR_AP_ARP_VLAN_NOT_SPECIFIED	2788	0xae4	VLAN must be specified while adding ARP entry within partition.
NSERR_AP_SHAREDVLAN_PART_EXIST	2789	0xae5	This VLAN already bound to the specified partition.
NSERR_PARTITION_ID_EXIST	2790	0xae6	Partition-id is already in use by another partition.
NSERR_SYNCNSVLAN_AP	2791	0xae7	VLAN bound to Admin Partition cannot be configured as SYNC/NS VLAN.

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_AP_NSVLAN	2792	0xae8	NSVLAN cannot be bound to Admin Partition.
NSERR_VXLAN_VLAN_DIFF_PARTITION	2799	0xaef	VXLAN and VLAN belong to different partitions.
NSERR_AP_VXLAN_TUNNEL_NOT_ALLOWED	2800	0xaf0	IPtunnel of type vxlan cannot be configured in non-default partition
NSERR_VXLAN_CONFIG_INPART	2801	0xaf1	This vxlan config not supported in non-default partition.
NSERR_VXLAN_OTHER_PARTITION	2802	0xaf2	Specified vxlan is already bound to some other partition.
NSERR_VXLAN_VLAN_BIND	2803	0xaf3	When vxlan extends vlan, these operations should be done on vlan
NSERR_VXLAN_IP_BINDING_CURPART	2804	0xaf4	IP binding to vxlan should be done in vxlan partition alone
NSERR_VXLAN_BOUNDTO_PARTITION	2805	0xaf5	Specified vxlan is already bound to the partition.
NSERR_DYNROUTING_PARTITION	2806	0xaf6	Dynamic Routing should be enabled or disabled in vlan/ vxlan partition

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_AP_SHAREDVLAN_VXLAN	2807	0xaf7	Shared vlan cannot be bound/unbound to/from a vxlan.
NSERR_AP_VLAN_VXLAN_EXIST	2808	0xaf8	The specified VLAN cannot be shared to a partition because it is extended by a vxlan .
NSERR_AP_STATIC_ARP_ND6_VXLAN_NOT_ALLOWED	2809	0xaf9	Static arp/nd6 entries cannot be added with vxlan in non-default partition
NSERR_AP_MEM_MIN_LIMIT	2810	0xafa	Partition's memory limit cannot be less than 5MB
NSERR_AP_BDGGRP_BINDING_NOT_ALLOWED	2811	0xafb	The specified BridgeGroup cannot be bound to a partition because one of its member VLAN is configured as untagged member of interface.
NSERR_AP_NOT_LOCAL_ADMIN_PMAC	2812	0xafc	Local-admin bit must be set for Partition MAC address.
NSERR_AP_NOMEM	2813	0xafd	Cannot allocate memory. The total memory budgeted across all partitions will exceed the system capacity.

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_AP_SHARE DVLAN_ROUTING_ NOT_ALLOWED	3035	0xbdb	Dynamic routing not allowed on shared vlan in non default partition
NSERR_AP_LOW_ MEM_LIMIT	3036	0xbdc	The recommended minimum amount of memory is 50 MB. Allocate more memory for this partition.

PBR ERRORS

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_PBR_NEXT HOP_NOTDIRECT	912	0x390	PBR Nexthop should be direct
NSERR_PBR_NOL OOPBACK	913	0x391	PBR cannot be configured on the loopback interface
NSERR_PBRDELER ROR	914	0x392	This PBR has already been removed
NSERR_PBR_IPPIP _EXISTS	915	0x393	PBR with identical parameter specification already exists
NSERR_PBR_PRIO RITY_EXISTS	916	0x394	PBR with this priority already exists
NSERR_PBRMODC FGINFO	918	0x396	PBR modified, use 'apply pbrs' to commit this operation

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_PBR_NEXTHOP_REQD	919	0x397	PBR Nexthop is required
NSERR_PBR_L2_CONFIG_INFO	920	0x398	L2 based PBRs work only for routed traffic
NSERR_PBRMODCFG_L2_INFO	921	0x399	L2 based PBRs work only for routed traffic: PBR modified, use 'apply pbrs' to commit this operation
NSERR_PBR_NO_MONITOR_GATEWAY	922	0x39a	Monitor can't be configured when nexthop is configured as gateway name
NSERR_PBR_INVALID_IPORGATEWAY	923	0x39b	Invalid Nexthop IPaddress/Gateway name
NSERR_PBR_MAX_RULE_EXCEEDED	924	0x39c	Number of PBRs on the system exceeds Maximum
NSERR_PBR_NEXTHOP_TUNNEL_REQD	925	0x39d	PBR Nexthop or IpTunnel is required
NSERR_PBR_DENY_MSR	926	0x39e	MSR cannot be enabled on PBR with DENY config
NSERR_ACL_MAC_MASK_INVALID	927	0x39f	SrcMacMask should contain only 1/0s, use 0s for matching and 1s for not matching

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_PBR_IPSEC_ALREADY_BOUND	1445	0x5a5	Use IKEv1 in IPSec profile. For IPSEC tunnels with IKEv2, Only one PBR is allowed to be bound to a tunnel
NSERR_PBR_REMOVED	1446	0x5a6	PBR is removed
NSERR_PBR_L2PARAM_GRE	1456	0x5b0	PBR is having L2PARAM. Cannot have GRE as nexthop.
NSERR_PBR_VXLAN	1457	0x5b1	VXLAN cannot be a nexthop.
NSERR_PBR_TUNNELBOUNDTONETBRIDGE	933	0x3a5	Tunnel is already bound to Netbridge
NSERR_PBR_SETNEXTHOP_TUNNEL	1217	0x4c1	Tunnel is bound to PBR. Cannot set NextHop
NSERR_ACL_PBRMODCFGINFO	2445	0x98d	ACL/PBR modified, use 'apply acls/pbrs' to commit this operation

PBR6 ERRORS

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_PBR6_IPPIP_EXISTS	880	0x370	PBR6 with identical parameter specification already exists

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_PBR6_DELERROR	881	0x371	PBR6 has already been removed
NSERR_PBR6_ADDERROR	882	0x372	Port can be specified only if protocol is TCP (6) or UDP (17)
NSERR_PBR6_PRIORITY_EXISTS	883	0x373	PBR6 with this priority already exists
NSERR_PBR6_ICMP_REQD	884	0x374	ICMPv6 type/code can be specified only if protocol is ICMPv6 (1)
NSERR_PBR6_UNSPECADDR	885	0x375	unspecified address (::) can not be configured in PBR6
NSERR_PBR6_MODCFGINFO	886	0x376	PBR6 modified, apply pbr6 to activate change
NSERR_PBR6_PREFIXLEN	887	0x377	Prefix length should not be configured in PBR6. (Use range instead)
NSERR_PBR6_SPECIFY_NEXTHOPVLAN	888	0x378	Nexthop VLAN should be specified with Link local gateway address
NSERR_PBR6_INVALID_GATEWAY	889	0x379	Invalid PBR6 Gateway
NSERR_PBR6_INVALID_NEXTHOP_VLAN	890	0x37a	Invalid Nexthop VLAN ID

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_PBR6_MAX_RULE_EXCEEDED	891	0x37b	Number of PBR6s on the system exceeds Maximum

PCP ERRORS

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_PCP_PROFILE_BOUND	3521	0xdc1	Cannot remove PCP Profile. To remove PCP profile, first unset it from PCP servers
NSERR_PCPPROFILE_NOT_EXIST	3522	0xdc2	PCP profile does not exist, use 'show pcp profile' to check available pcp profiles
NSERR_LSNPCP_BINDING_EXIST	3523	0xdc3	Please unbind existing PCP server from lsn group
NSERR_PCPSERVER_NOT_EXIST	3524	0xdc4	PCP server does not exist, use 'show pcp server' to check available pcp servers
NSERR_PCPSERVER_BIND_EXIST	3525	0xdc5	Can not Remove PCP server. Please unbind pcp server from all bindings
NSERR_PCPSERVER_INVALID_IP	3526	0xdc6	PCP Server IP Should be SNIP.
NSERR_PCP_LIFE_TIME	3527	0xdc7	PCP Min life time is greater than Max life time.

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_PCPSERVER_LSNGROUP_TYPE_DIFF	3528	0xdc8	PCP Server being bound is incompatible with the LSN group.

PI ERRORS

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_PI_LONGVSVRNAME	3040	0xbe0	The name of the label must be less than 32 characters
NSERR_PI_PRIORITY_EXISTS	3041	0xbe1	A policy is already bound to the specified priority
NSERR_PICON_GOTO_NOT_END	3042	0xbe2	GotoPriorityExpression for this policy has to be END
NSERR_INVAL_THRESHOLD	3043	0xbe3	Invalid threshold size value. Threshold size must be lesser than the sample size
NSERR_DEF_INVALID_UNBIND	3044	0xbe4	Default binding cannot be unbound
NSERR_BAD_INIT_VALUE	3045	0xbe5	Invalid initial value
NSERR_INIT_VALUE_TOO_BIG	3046	0xbe6	Initial value is larger than the maximum allowed text length and the ifValueTooBig action is undef

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_INIT_VALUE_TRUNCATED	3047	0xbe7	Initial value has been truncated to the maximum allowed text length because the ifValueTooBig action is truncate
NSERR_BAD_ASSIGN_LHS	3048	0xbe8	Invalid -var parameter: expect $variable-name for a ulong or text variable or $variable-name[key-expression] for a map variable.
NSERR_BAD_OP_FOR_TYPE	3049	0xbe9	Op is not allowed for the variable type.
NSERR_BAD_VAR_TYPE	3050	0xbea	Invalid type: expected one of ulong, text, or map.
NSERR_ASSIGNMENT_LOG_UNSUPPORTED	3051	0xbeb	Log action is not supported with assignment action
NSERR_UNDEF_EXCEPTION	3052	0xbec	Undef exception raised.
NSERR_NO_VARIABLE_VALUE	3053	0xbed	No value exists for the variable and key.
NSERR_BAD_KEY_TYPE	3056	0xbf0	Invalid key type: expected type text
NSERR_BAD_SINGLETON_VAR	3057	0xbf1	Not a singleton variable

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_BAD_MAP_VAR	3058	0xbf2	Not a map variable
NSERR_UNKNOWN_VARIABLE	3059	0xbf3	Variable is not configured.
NSERR_MAP_WITHOUT_KEY	3060	0xbf4	Map variable used without a key.
NSERR_SINGLETON_WITH_KEY	3061	0xbf5	Singleton variable used with a key.
NSERR_BAD_TEXT_MAX_LENGTH	3062	0xbf6	Invalid text type: expected text(max-length), where max-length is an unsigned integer >= 1 and <= 64000.
NSERR_BAD_MAP_TYPE_SYNTAX	3063	0xbf7	Invalid map type: expected map(key-type, value-type, max-entries), where max-entries is an unsigned long value <= 18446744073709551615 and greater than 0.
NSERR_BAD_MAP_KEY_TYPE	3064	0xbf8	Map key type must be text.
NSERR_BAD_MAP_VALUE_TYPE	3065	0xbf9	Map value type must be ulong or text.
NSERR_BAD_KEY_VALUE_LENGTH	3066	0xbfa	Sum of the maximum map key and value lengths must be <= 64000.

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_BAD_MAP_SET_TYPE	3067	0xbfb	Invalid type parameter for set.
NSERR_TRANSACTION_MAPS_NOT_SUPPORTED	3068	0xbfc	Maps with transaction scope are not supported.
NSERR_TRANSACTION_EXPIRE_NOT_SUPPORTED	3070	0xbfe	Expiration with transaction scope variables is not supported.
NSERR_INVOKE_NOT_SUPPORTED	3071	0xbff	Policy does not support invoke.
NSERR_INVALPIEXPR	3073	0xc01	Invalid expression
NSERR_INVALINTOP	3074	0xc02	Expecting numeric arguments in this context for '-', '+', '*' or '/'
NSERR_INVALCOMPARE	3075	0xc03	Invalid arguments to compare operation
NSERR_INVALBOOLOP	3076	0xc04	The '!', '||' and ';;' operators can have only Boolean argument(s)
NSERR_ARGNEG	3077	0xc05	Argument cannot be negative
NSERR_ARGEXCEED	3078	0xc06	Argument exceeds maximum allowed value

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_ARGZERO	3079	0xc07	Operand or function argument should be non-zero
NSERR_MAXHEADER	3080	0xc08	Number of custom header exceeds limit
NSERR_INVALPICEXPR	3081	0xc09	Expression syntax error
NSERR_CEXPRLIMIT	3082	0xc0a	Expression too long
NSERR_EXPRLIMIT	3083	0xc0b	Expression too long
NSERR_SEXPRLIMIT	3084	0xc0c	String expression too long
NSERR_INVALPISEXPR	3085	0xc0d	String expression syntax error
NSERR_NOBIDI	3086	0xc0e	Bi-directional expression not allowed
NSERR_NOLAB	3087	0xc0f	Policy Label does not exist
NSERR_INTERNAL_LABEL_RM	3088	0xc10	Default Policy labels cannot be removed
NSERR_POLICY_FLOWTYPE_NONE	3089	0xc11	Policy should either be a request or response policy
NSERR_INVAL_PRIORITY	3090	0xc12	Priority is mandatory for advanced expressions and should be in the

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
			range from 1 to 2147483647
NSERR_NUMERICEXPR	3091	0xc13	Expression should evaluate to numeric value
NSERR_BOOLEXPR	3092	0xc14	Expression should evaluate to true or false
NSERR_NOTBOUND	3093	0xc15	Cannot unbind a policy that is not bound
NSERR_POLICY_INUSE	3094	0xc16	Policy name already in use
NSERR_POLICY_SET_NOTALLOWED	3095	0xc17	Invalid rule/action for bound policy
NSERR_INVALID_BIND	3096	0xc18	Policy cannot be bound to specified policy label
NSERR_USE_INVOKE_RESULT	3097	0xc19	USE_INVOCATION_RESULT can be used only with invoke
NSERR_INVAL_EXPR_DATA_TYPE	3098	0xc1a	Invalid expression data type
NSERR_EXPR_CONST_ONLY	3099	0xc1b	Only constant parameters are allowed for function
NSERR_ALT_EXPR_STRING_ONLY	3100	0xc1c	Only string expressions are allowed for ALT

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_ACTION_DEF_SET_INVAL	3101	0xc1d	Default action cannot be modified
NSERR_POLICY_DEF_SET_INVAL	3102	0xc1e	Default policy cannot be modified
NSERR_POLICY_LABEL_DEF_SET_INVAL	3103	0xc1f	Default policylabel cannot be modified
NSERR_INVAL_UNBIND	3104	0xc20	Policy not bound to specified policy label
NSERR_REGEX_INVALID	3105	0xc21	Invalid regular expression
NSERR_REGEX_BACKREF	3106	0xc22	Backreference in regular expression
NSERR_REGEX_RECURSIVE	3107	0xc23	Recursive regular expression present
NSERR_PIXL_EXPR_UNSAFE	3108	0xc24	Input expression is unsafe
NSERR_PI_ACTION_MAX_REF_REACHED	3109	0xc25	Cannot create policy. Binding limit for action reached (65536)
NSERR_PI_INVALID_UNSET	3110	0xc26	Cannot unset rule or action. No changes done
NSERR_EMPTY_STRING	3111	0xc27	Zero length string not allowed
NSERR_INVAL_BTW_ARGS	3112	0xc28	Arguments to BETWEEN are incorrect

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_INVAL_ARG_SPECIFIED	3113	0xc29	GotoPriorityExpression, flowtype and invoke apply only to rewrite, responder and cache policies
NSERR_INVAL_ARG_CSPL	3854	0xf0e	Target vserver cannot be specified along with GotoPriorityExpression and invoke.
NSERR_FLOWTYPE_NOT_APPLICABLE	3114	0xc2a	Flowtype applies only to rewrite, responder and cache policies
NSERR_INVAL_ARG_SPECIFIED_CS	3115	0xc2b	Flowtype and invoke apply only to Advanced policies.
NSERR_INVAL_GOTOEXPR_CS	3116	0xc2c	GotoPriorityExpression applies only to Advanced policies
NSERR_REBIND_FAILED	3117	0xc2d	Rebinding of policy with new bind parameters failed. The policy is unbound.
NSERR_SECOND_BIND	3118	0xc2e	A policy can be bound only once
NSERR_NONHTTP_VS	3119	0xc2f	Specified policy can be bound only to HTTP/SSL/PROXY/HTTP_QUIC vserver

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_PI_LEX_FAILURE	3344	0xd10	Error in parsing
NSERR_COMPAT_RESULT_TYPES	2889	0xb49	Result expression types must be compatible
NSERR_PI_INVALID NAME	3856	0xF10	Invalid policy entity name: names must begin with an ASCII alphabetic character or underscore and must contain only ASCII alphanumerics or underscores; words reserved for policy use may not be used
NSERR_PI_RST_CONN	3855	0xF0F	Message processing reset connection
NSERR_PI_EXPR_CSMSG	3857	0xF11	Advanced expression cannot have client security message
NSERR_INVAL_XPATH_EXPR	3858	0xf12	XPath Expression Compilation Failed
NSERR_XPATH_EXPR_NOT_SUPPORTED	3859	0xf13	Unsupported XPath
NSERR_TARGET_INVAL	3860	0xf14	Target Vserver cannot be specified for this policy
NSERR_NON_RESP_HTTP_VS_LIST	3861	0xf15	Specified policy can be bound only to HTTP/SSL/

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
			HTTP_QUIC/TCP/ SSL_BRIDGE/FTP/ DNS_TCP/RTSP/ SSL_TCP/NNTP/ MSSQL/MySQL/ ORACLE/ DIAMETER/ RADIUS/ANY/ PROXY/MQTT/ MQTT_TLS/UDP vserver
NSERR_INVAL_VSERVER_BIND	3862	0xf16	Policy can be bound only to LB/CS vserver types
NSERR_APP_FREED_NSB	3863	0xf17	Application reset/ drop connection and freed nsb
NSERR_MULT_BIND_INVAL	3864	0xf18	CVPN Policies cannot be bound to multiple entities
NSERR_CLASSIC_POLICY_ALREADY_BOUND	3865	0xF19	Cannot bind an advanced policy to a virtual server to which a classic policy is already bound
NSERR_ADVANCED_POLICY_ALREADY_BOUND	3872	0xF20	Cannot bind a classic policy to a virtual server to which an advanced policy is already bound
NSERR_MULT_UNBIND	3873	0xF21	Policy is bound to multiple global bindpoints. Please

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
			specify the appropriate bindpoint to unbind it.
NSERR_UNKNOWN_CERTKEY	3874	0xF22	The specified certkey object has not been configured
NSERR_NO_RSA_PUBLIC_KEY	3875	0xF23	The specified certkey object does not include a certificate with an RSA public key
NSERR_NO_RSA_PRIVATE_KEY	3876	0xF24	The specified certkey object does not include an RSA private key
NSERR_CERTKEY_NAME_TOO_LONG	3877	0xF25	The certkey name exceeds the maximum 63 characters
NSERR_INVALID_UTF_8	3878	0xF26	Invalid UTF-8 string
NSERR_UNRECOG_CHARSET	3879	0xF27	Unrecognized character set
NSERR_INCOMPATIBLE_NAME_EXPR_CHANGE	3880	0xF28	Incompatible named expression change for in-use expression.
NSERR_HEADER_EXPR_ONLY	3881	0xF29	Only classic expressions for headers allowed in EVAL_CLASSIC_EXPR

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_RW_NOT_SUPPORTED_VS	3904	0xF40	Specified policy can be bound only to HTTP/SSL/ HTTP_QUIC/TCP/ SSL_TCP/ DIAMETER/ SSL_DIAMTER/ SIP_UDP/RADIUS/ PROXY vserver
NSERR_INVALID_KEYVALUE	3905	0xf41	The keyvalue argument is incorrect.
NSERR_INVALID_RESOURCE_NAME	3906	0xF42	Resource of the given name does not exist
NSERR_INVALID_ACTION	3907	0xF43	Invalid action
NSERR_INVALID_ENUM_VALUE	3909	0xF45	Invalid enumeration value
NSERR_INVALID_BINDPOINT	3910	0xF46	Invalid bind point.
NSERR_NO_FIPS_FOR_POLICY_CRYPTO	3911	0xF47	A FIPS key cannot be used for policy crypto functions.
NSERR_NO_CONFIGDB_DATA_SELECTED	3912	0xF48	No data selected from the configuration database.
NSERR_HEADER_NAME_LENGTH_LIMIT	3913	0xF49	Custom header name is too long.

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_UNSUPPORTED_CVPN_SEARCH	3914	0xF4A	Patset, dataset, and xpath not supported for clientless VPN search.
NSERR_INVALID_HEADER_NAME	3915	0xF4B	Header name contains invalid characters (one or more of ( ) < > @ , ; : \\ \" / [ ] ? = { } and space) as per the HTTP spec RFC 2616. This is allowed to for non-conformant HTTP messages, but may not be what you intended.
NSERR_HEADER_NAME_TOO_LONG	3916	0xF4c	Header name is too long (maximum of 32 characters allowed).
NSERR_CSACTION_NOT_SUPPORTED	3918	0xF4E	Content Switching actions are not supported for classic content switching policies.
NSERR_PI_EXPR_TOO_BIG	3919	0xF4F	Expression too long - maximum length is 8191
NSERR_PI_INVALID_FUNCTION_NAME	3946	0xF6A	Cannot use Advanced Expression reserved word as a function name.

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_PI_FUNCTION_NAME_EXISTS	3947	0xF6B	Function with the same name already exists.
NSERR_EXTENSION_INVALID_UPDATE_NAME	3948	0xF6C	Add the extension before updating.
NSERR_PI_INVALID_EXTENSION_NAME	3949	0xF6D	Extension is not added.
NSERR_EXTENSION_FUNCTION_PROTOTYPE_CHANGED	3950	0xF6E	Extension has different prototype of a function than that which is in use.
NSERR_EXTENSION_FUNCTION_UPDATE_PROBLEM	3951	0xF6F	Problem in updating function that is in use.
NSERR_EXTENSION_COMPILE_FAILURE	3962	0xF7A	Extension compilation error.
NSERR_EXTENSION_LOAD_FAILURE	3963	0xF7B	Extension loading error.
NSERR_PI_USED_FUNCTION_REMOVED	3964	0xF7C	Update attempted to remove a function that is in use.
NSERR_EXTENSION_FUNCTION_MULTIPLE_DEFINITIONS	3965	0xF7D	Extension has multiple definitions of a function.
NSERR_EXTENSION_INVALID_FUNCTION_PROTOTYPE	3966	0xF7E	Extension function's prototype is invalid.

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_EXTENSION_MAX_FUNCTION_ARGUMENT	3967	0xF7F	Maximum number of function arguments can be 3.
NSERR_BAD_EXTENSION_TRACE_NAME	4038	0xFC6	Function or variable name can contain only alphanumerics and underscores and cannot begin with a digit.
NSERR_BAD_EXTENSION_TRACE_ARRAYS	3024	0xBD0	traceFunctions or traceVariables cannot be specified with trace off.
NSERR_PI_INVALID_GLOBAL_BINDTYPE	3828	0xEF4	Invalid global bindtype.
NSERR_INVALID_POLICY_GLOBAL_BINDING	3829	0xEF5	Policy cannot be bound/unbound to/ from the given global bindtype.
NSERR_INVALID_PI_ANNOTATE	1465	0x5b9	Invalid Advanced Expression annotation value
NSERR_INVALID_PI_ANNOTATE_LOGINSCHEMA	1466	0x5ba	Invalid loginSchema corresponding to Advanced Expression annotation value
NSERR_ANGLE_BRACKETS_IN_TAGNAME	3830	0xEF6	Invalid syntax, angle brackets in tag specified

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_INVALID_ENCRYPTION_KEY_ARGUMENT	3831	0xEF7	Invalid encryptionKey argument
NSERR_INVALID_HMAC_KEY_ARGUMENT	3832	0xEF8	Invalid hmacKey argument
NSERR_ENCRYPTION_KEY_NOTPRESENT	3833	0xEF9	Encryption key does not exist.
NSERR_HMAC_KEY_NOTPRESENT	3834	0xEFA	HMAC key does not exist.
NSERR_WARN_SHORT_HMAC_KEY	3835	0xEFB	Recommend that the HMAC keyValue be at least as long as the digest blocksize
NSERR_MULT_TYPE_UNBIND	3836	0xEFC	Please specify the appropriate bindpoint to unbind.
NSERR_EMPTY_CERTKEY	3837	0xEFD	The specified certkey name is empty or NULL.
NSERR_NON_SSL_HTTP_VS	3838	0xEFE	Specified policy can be bound only to HTTP/SSL vserver
NSERR_EXTENSION_HAS_GENERIC_MBLB_API_NOT_FUNCTION_API	3839	0xEFF	Extension code already used for an Advanced Expression extension function cannot be used for a user protocol implementation.

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_EXTENSION_HAS_FUNCTION_API_NOT_GENERIC_MBLB_API	3424	0xD60	Extension code already used for a user protocol implementation cannot be used for an Advanced Expression extension function.
NSERR_EXTENSION_INCORRECT_USER_PARAM_VALUE	3435	0xD6B	Incorrect parameter field's value. Value should be in = format.
NSERR_EXTENSION_USER_PROTOCOL_IN_USE	1502	0x5DE	Can't update the extension as the user protocol using this extension is in use
NSERR_USER_VSERVER_EXCEED_PARAM_NAME_VALUE_LENGTH	1503	0x5DF	Parameter's name or value length exceeds maximum allowed length of 63 characters
NSERR_USER_VSERVER_INVALID_DEFAULT_LB_PROTOCOL_TYPE	2832	0xB10	Default Load Balancing virtual server's protocol type should be a user type.
NSERR_USER_VSERVER_DIFFERENT_TRANSPORT_DEFAULT_LB_PROTOCOL_TYPE	2831	0xB0F	Transport type and default Load Balancing virtual server's protocol type are not compatible.

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_INTERIM_UPDATE_SUPPORT_IN_RADIUS_ONLY	3436	0xD6C	Treat Radius Interim message as Start message is only supported in Radius-Only mode.
NSERR_WARN_VAR_SET_INIT	3437	0xD6D	Set of the init parameter will not affect existing variable values.
NSERR_CI_UNSUPPORTED_VS	3454	0xD7E	A Content Inspection policy can be bound only to LB vservers of type HTTP and SSL, and CS vservers of type HTTP, SSL and PROXY
NSERR_CI_ICAP_FLOWTYPE_MISMATCH	3470	0xD8E	This Content Inspection policy's ICAP action is incompatible with the specified bindpoint
NSERR_INVALID_POLICY_BINDING	3438	0xD6E	Policy cannot be bound/unbound to/ from this vserver for the given bindtype.
NSERR_HTTP_REQ_USER_DEPRECATED	3456	0xD80	HTTP.REQ.USER has been deprecated. Use AAA.USER instead.
NSERR_ASSIGN_CONTEXT_NOT_PRESENT	3471	0xD8F	Assignment attempted when not in a connection context.

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_SELFAUTH_DEPRECATED	3481	0xD99	Selfauth as ssotype has been deprecated.
NSERR_RHS_TARGET_REQUIRED	3482	0xD9A	TARGET is required in the rewrite action stringBuilder expression when a refineSearch expression contains a REGEX or XPATH function.
NSERR_AAA_GRP_AS_XML_DEPRECATED	3483	0xD9B	GROUPS_AS_XML has been deprecated. Use AAA.USER.GROUPS instead.
NSERR_REDIRECT_URL_SAML	3484	0xD9C	Redirect URL is a required argument for adding SAML action. Please specify it explicitly, or enter Metadata URL from which it can be imported.
NSERR_CI_IPS_FLOWTYPE_MISMATCH	3486	0xD9E	Policy's action is incompatible with specified bindpoint or flow type
NSERR_SAML_ACT_CONF_ISSUE	3487	0xD9F	Saml configuration failure as samlIdPCertName/ samlRedirectUrl present when meatadataURL is provided

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_PATFILE_REF_EXIST	1964	0x7AC	The specified patset file is already associated with a patset/dataset
NSERR_PATSET_PATSETFILE_REFERENCE	2033	0x7F1	Cannot bind/unbind patterns for a patset/dataset with patsetfile association
NSERR_INVAL_LB_VSERVER_BIND	2288	0x8f0	Policy can be bound only to LB/GSLB vserver types
NSERR_INVALID_UNBINDPOINT	2294	0x8f6	Invalid flowtype for unbind

POL ERRORS

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_INVALIDPOL	2053	0x805	Binding invalid policy
NSERR_NOPOL	2054	0x806	No such policy exists
NSERR_RULEURL	2055	0x807	Rule or URL required
NSERR_DELMC	2056	0x808	Delay or maxConn argument required
NSERR_ACP	2057	0x809	Alternate content path not required
NSERR_ACS	2058	0x80A	Alternate content service not required

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_NOSET_CEXP	2059	0x80B	No support to set compound expression value
NSERR_CEXP_DEPTH	2060	0x80C	Maximum recursive depth reached
NSERR_NOVPNAPP	2061	0x80D	No such intranet application exists
NSERR_NOSET_CSE	2062	0x80E	Changing rule to/ from client security expression is not allowed when policy is in use
NSERR_INVAL_POLNAME	2063	0x80F	Invalid policy Name
NSERR_UNBIND_INVALIDPOL	2097	0x831	Policy not bound
NSERR_EXCEED_MAX_POL_LIMIT	2098	0x832	32 authentication policies are already bound
NSERR_INTERNAL_PI_ERROR	2103	0x837	Internal policy error
NSERR_NEG_POL_VIOL1	2104	0x838	Only negotiate and certificate policies can be bound together
NSERR_NEG_POL_VIOL2	2105	0x839	Negotiate policy in primary can be bound only along with ldap policy (with authentication turned off) in secondary

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_NEG_POL_VIOL3	2106	0x83A	Negotiate policy in secondary can be bound only along with certificate policy in primary
NSERR_SAML_POL_VIOL1	2122	0x84A	SAML policy can only be the last in the cascade or the only one in the cascade
NSERR_SAML_POL_VIOL2	2123	0x84B	SAML policy in primary can be bound only along with ldap policy (with authentication turned off) in secondary
NSERR_SAML_POL_VIOL3	2124	0x84C	SAML policy cannot be bound to secondary cascade
NSERR_SAML_DISABLED	2125	0x84D	SAML policy binding is disabled
NSERR_LDAP_POL_VIOL1	2088	0x828	Only LDAP policies may be bound for group extraction.
NSERR_LDAP_POL_VIOL2	2089	0x829	An LDAP policy bound for group extraction must set -authentication DISABLED.
NSERR_NON_SELECTOR_POLICY	2107	0x83B	Only selector based policies can be bound to sql vserver

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_BAD_SELECTOR	2108	0x83C	Selector does not match content group type
NSERR_BAD_CONTENTGROUP	2109	0x83D	Contentgroup not compatible
NSERR_SQL_POL_GLOBAL_BINDPOINT	2110	0x83E	Datastream cache policies cannot have global/override bindpoint
NSERR_APPQOE_INVALID_ACP	2111	0x83F	Alternate content path is invalid
NSERR_APPQOE_CLTRATE	2086	0x826	Client detect rate is not required
NSERR_APPQOE_DOSTHRESH_NREQ	2087	0x827	DoS attack threshold is not required
NSERR_APPQOE_DOSTHRESH_REQ	2090	0x82a	DoS attack threshold is required
NSERR_APPQOE_ACS_REQ	2091	0x82b	Alternate content service is required
NSERR_APPQOE_ACP_REQ	2092	0x82c	Alternate content path is required with alternate content service
NSERR_APPQOE_VSVR_CONFIG_CONFLICT	2094	0x82E	AppQoE policy cannot be bound to vserver configured for PQ/SC

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_APPQOE_SVC_CONFIG_CONFLICT	2095	0x82F	AppQoE policy cannot be bound to vserver with services configured for SC/HDOSP
NSERR_APPQOE_UNSUPPORTED_PROTO	2142	0x85E	Specified policy can be bound only to HTTP/SSL/HTTP_QUIC vserver
NSERR_APPQOE_UNSUPPORTED_VSVR	2143	0x85F	Specified policy can be bound only to LB vserver types
NSERR_CLASSIC_POLICY_INVALID_ARG	2145	0x861	Invalid arguments for classic policy binding
NSERR_AUTHN_ADVANCE_INVALID_ARG	2146	0x862	Invalid arguments for advanced authentication policy binding
NSERR_RENAME_NOT_PERMITTED	2147	0x863	Rename operation not permitted
NSERR_PI_AUTHZPLCY_NOT_SUPPORTED	2148	0x864	advanced authorization policy cannot be bound to aaa user/group
NSERR_SAML_2FACTOR_CONFLICT	2149	0x865	SAML 2-Factor policy should always be at the beginning of cascade
NSERR_AUDIT_SYSADVPLCY_BOUND	2150	0x866	Cannot bind Classic Syslog Policy to System global if Advanced Syslog

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
			Policy is already bound to SyslogGlobal
NSERR_AUDIT_SYSCLASSICPLCY_BOUND	2151	0x867	Cannot bind Advanced Syslog Policy to SyslogGlobal if Classic Syslog Policy is already bound to System Global
NSERR_CLASSIC_TMSESSPOL_ALREADY_BOUND	2152	0x868	Advanced TM Session Policy cannot be bound if Classic TM Session Policy is already bound to any entity (i.e. aaa user, aaa group, authentication vserver, tm global)
NSERR_ADVANCED_TMSESSPOL_ALREADY_BOUND	2153	0x869	Classic TM Session Policy cannot be bound if Advanced TM Session Policy is already bound to any entity (i.e. aaa user, aaa group, authentication vserver, tm global)
NSERR_AUDIT_NSADVPLCY_BOUND	2311	0x907	Cannot bind Classic Nslog Policy to System global if Advanced Nslog Policy is already bound to NslogGlobal

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_AUDIT_NSCLASSICPLCY_BOUND	2312	0x908	Cannot bind Advanced Nslog Policy to NslogGlobal if Classic Nslog Policy is already bound to System Global
NSERR_CLASSIC_AUTHNPOL_ALREADY_BOUND	2219	0x8ab	Advanced authentication Policy cannot be bound if Classic authentication Policy is already bound to system global
NSERR_ADVANCED_AUTHNPOL_ALREADY_BOUND	2220	0x8ac	Classic authentication Policy cannot be bound if Advanced authentication Policy is already bound to system global
NSERR_NEXTFACTOR_ATTRIBMAP_MISMATCH	2221	0x8ad	Bind functionality not supported for current bind-entity and nextFactor
NSERR_CLASSIC_VPNTRAFFICPOL_ALREADY_BOUND	2222	0x8ae	Advanced VPN Traffic Policy cannot be bound if Classic VPN Traffic Policy is already bound to any entity (i.e. aaa user, aaa group, vpn vserver, vpn global)
NSERR_ADVANCED_VPNTRAFFICPO	2223	0x8af	Classic VPN Traffic Policy cannot be

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
L_ALREADY_BOUND			bound if Advanced VPN Traffic Policy is already bound to any entity (i.e. aaa user, aaa group, vpn vserver, vpn global)
NSERR_CLASSIC_AUTHPOL_ALREADY_BOUND	2224	0x8b0	Advanced Authorization Policy cannot be bound if Classic Authorization Policy is already bound to any entity (i.e. aaa user, aaa group)
NSERR_ADVANCED_AUTHPOL_ALREADY_BOUND	2225	0x8b1	Classic Authorization Policy cannot be bound if Advanced Authorization Policy is already bound to any entity (i.e. aaa user, aaa group)
NSERR_CLASSIC_VPNSESSPOL_ALREADY_BOUND	2226	0x8b2	Advanced VPN Session Policy cannot be bound if Classic VPN Session Policy is already bound to any entity (i.e. aaa user, aaa group, vpn vserver, vpn global)
NSERR_ADVANCED_VPNSESSPOL_ALREADY_BOUND	2227	0x8b3	Classic VPN Session Policy cannot be bound if Advanced VPN Session Policy is already bound to any entity (i.e. aaa

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
			user, aaa group, vpn vserver, vpn global)
NSERR_INVALID_AUTHN_SET_ACTION_SUBTYPE	2228	0x8b4	Setting action for advanced authentication policy not allowed for different action subtype
NSERR_CLASSIC_AUTH_POLICY_DEPRECATED	2229	0x8b5	Classic authentication policies are deprecated and will be removed in the next major release. Please use advanced authentication policies (i.e. add/set authentication policy)
NSERR_CLASSIC_PREAUTH_POLICY_DEPRECATED	2230	0x8b6	Classic Pre-authentication policies are deprecated and will be removed in the next major release. Please use advanced authentication policies (i.e. add/set authentication epaaction, add/set authentication policy)
NSERR_INVALID_POLICY_CONTAIN_CSEC	2231	0x8b7	Binding policy with Client Security expression is not

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
			allowed for ICAOnly VPN Virtual Server
NSERR_CLASSIC_AUDITLOGPOL_ALREADY_BOUND	2232	0x8b8	Advanced Audit Policy cannot be bound if Classic Audit Policy is already bound to Vserver
NSERR_ADVANCED_AUDITLOGPOL_ALREADY_BOUND	2233	0x8b9	Classic Audit Policy cannot be bound if Advanced Audit Policy is already bound to Vserver
NSERR_MAX_AUDITLOGPOL_REACHED	2234	0x8ba	Maximum auditlog policy binding to vserver reached
NSERR_PI_ADVANCED_POLICY_ALREADY_ADDED	2235	0x8bb	Failed to bind classic policy because advanced policy(s) is already bound.
NSERR_PI_CLASSIC_POLICY_ALREADY_ADDED	2236	0x8bc	Failed to bind advanced policy because classic policy(s) is already bound.
NSERR_CLASSIC_CLIENT_SECURITY_DEPRECATED	2237	0x8bd	Client security expressions are deprecated using this command. Please use advanced authentication policies (i.e. add/set authentication

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
			epaaction, add/set authentication policy)
NSERR_CLASSIC_VPNURLPOL_ALREADY_BOUND	2240	0x8c0	VPN URL Policy cannot be bound if Classic VPN URL is already bound to any entity
NSERR_ADVANCED_VPNURLPOL_ALREADY_BOUND	2241	0x8c1	Classic VPN URL cannot be bound if VPN URL Policy is already bound to any entity
NSERR_PORTALTHEME_DEPRECATED	2242	0x8c2	Default, GreenBubble and X1 themes will be deprecated in the future release. Please use RfWebUI theme or RfWebUI based custom theme
NSERR_METADATA_REFRESH_MAX_INTERVAL	2243	0x8c3	Max metadata refresh interval support has been changed to 3600 minutes (60 hours)
NSERR_EPA_V2_CONFIG_FAILED	2244	0x8c4	EPA V2 config failed. Reconfigure this epa action when EPA v2 is enabled

POOLED LIC ERRORS

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_POOLED_LIC_SET_CAP	3569	0xdf1	Unable to set capacity
NSERR_POOLED_LIC_LPED_COMM	3570	0xdf2	Connection to LPED failed
NSERR_POOLED_LIC_SERVER_CONN	3571	0xdf3	Unable to connect to licenseserver
NSERR_POOLED_LIC_BAD_STATE	389	0x185	License engine initialization in progress

PQ ERRORS

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_PQ_BINDVIP	1360	0x550	Cannot bind same priority policy to VIP
NSERR_PQ_INVALPRIO	1361	0x551	Invalid priority value
NSERR_PQ_2BIGRULE	1362	0x552	Rule argument too big
NSERR_PQ_INVALWT	1363	0x553	Invalid weight value
NSERR_PQ_POLEXIST	1364	0x554	Policy name already in use
NSERR_PQ_NOPOL	1365	0x555	No such PQ policy exists

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_PQ_2MANYREF	1366	0x556	Cannot remove a policy which is bound to VIP
NSERR_PQ_NOLBVIP	1367	0x557	No such LB vserver exists
NSERR_PQ_PHSCONFIG	1368	0x558	Cannot configure PQ on VIP if physical service has PQ configuration
NSERR_PQ_NOBIND	1369	0x559	Cannot unbind PQ Policy which is not bound

QOS ERRORS

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_QOS_64BIT_NOT_SUPPORTED	3776	0xec0	Libqos is not currently supported on 64 bit platforms.
NSERR_QOS_FEATURE_LOCKED	3777	0xec1	QoS featuremask parameter cannot be used with the videooptimization feature enabled.

QUIC ERRORS

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_QUIC_INVALID_SERVER_ID	1699	0x6a3	Invalid hex format of custom server id. Length should be

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
			even and it must be a hex string
NSERR_QUIC_INVALID_CONFIG	1700	0x6a4	Invalid configuration

RESPOINT ERRORS

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_TECHSPRT_BUNDLE_MISSING	3824	0xef0	Tech support bundle does not exist.
NSERR_TECHSPRT_REMOVE	3825	0xef1	Error while removing tech support bundle.
NSERR_RESPOINT_MISSING	3826	0xef2	Restore point does not exist.
NSERR_RESPOINT_NAMEMISSING	2576	0xa10	Missing restore point name argument in the input.
NSERR_RESPOINT_MAXLIMIT	2577	0xa11	Reached max limit of 3 for restore points. Remove older restorepoints to proceed.
NSERR_CREATE_RESPOINT	2578	0xa12	Error while creating restore point.
NSERR_UPDATE_MAPFILE	2579	0xa13	Error while Updating the restorepoint map file.

REWRITE ERRORS

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_RW_ACT_INVAL	2817	0xb01	Invalid rewrite action
NSERR_RW_UNDEFACT_INVAL	2818	0xb02	Invalid undef action or log action
NSERR_ACTFLOWMISMATCH	2819	0xb03	Flow types of target and string expression are incompatible
NSERR_RONLY_TAR_EXPR	2820	0xb04	Target must be a simple reference to an unmodified portion of the message
NSERR_DATASET_BINDFAIL	2821	0xb05	Unable to bind the pattern to dataset/patset
NSERR_DATASET_UNBINDFAIL	2822	0xb06	Pattern or range does not exist in dataset/patset
NSERR_DATASET_NOTPRESENT	2823	0xb07	Dataset/Patset does not exist
NSERR_RSP_ACT_INVAL	2824	0xb08	Invalid responder action
NSERR_RSP_POLICY_FLOWTYPE_REQ	2825	0xb09	Responder policy must be a request policy
NSERR_TAR_FLOWTYPE_NRES	2826	0xb0a	Flow type of target should not be response type

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_RSP_CONFIG_LOCK	2827	0xb0b	Responder configuration is temporarily disabled
NSERR_RSP_ACT_MUST_BE_NOOP	2828	0xb0c	Non-terminating policy must have NOOP action
NSERR_PATSET_INVALID_REGEX	2829	0xb0d	Patset contains invalid regex.
NSERR_DATASET_BINDFAIL_DUP_INDEX	2830	0xb0e	Pattern index already in use, try using another index
NSERR_PATSET_BINDFAIL_PATLEN_LT_WU_MINLEN	2833	0xb11	Patset search on a body target not allowed if any of the patset patterns are < 3 or > 112 bytes in length, or a range is bound to the dataset
NSERR_TARGET_NOT_ALLOWED_IN_RULE	2834	0xb12	Expression involving Target not allowed in rule.
NSERR_RW_TARGET_NOT_ALLOWED_IN_STRBUILDER	2835	0xb13	Expression involving Target not allowed in StringBuilder expression.
NSERR_PIT_INVAL	2836	0xb14	Invalid Packet data
NSERR_INVAL_INVOKEPOINT	2837	0xb15	Invalid invoke point
NSERR_PIT_MAX_PACKET	2838	0xb16	Packet size exceeds maximum size

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_REFINE_SEARCH_INVALID	2839	0xb17	Regular expression for patterns not allowed when refine search is specified
NSERR_EXTEND_INVALID	2840	0xb18	Extend not allowed for non-body expressions
NSERR_NON_EXTEND_EXPR	2841	0xb19	Non extend expressions are not allowed
NSERR_EXTEND_INVAL_PIRL	2842	0xb1a	Extend not allowed in the string builder expression
NSERR_INVAL_TAR_EXPR	2843	0xb1b	Invalid target expression
NSERR_INVAL_SEARCH_ARGS	2845	0xb1d	Invalid argument: search supports text, xpath, xpath_json, xpath_html, regex and patset
NSERR_RSP_ACT_MUST_BE_RESET_DROP	2846	0xb1e	Policy action must be DROP|RESET
NSERR_INVAL_SEARCH_SYNTAX	2847	0xb1f	Invalid search syntax
NSERR_INVAL_SEARCH_XPATH_SYNTAX	2848	0xb20	Invalid xpath syntax
NSERR_INVAL_SEARCH_PATSET_SYNTAX	2849	0xb21	Invalid patset syntax

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_INVAL_SEARCH_REGEX_SYNTAX	2850	0xb22	Invalid regex syntax
NSERR_RW_REQ_BODY_NOT_ALLOWED	2851	0xb23	Request body based expression is not allowed
NSERR_RENAME_NOTSUPPORTED	2852	0xb24	Renaming this entity is not supported as entity based expression is configured
NSERR_ENTITY_REMOVAL_NOTALLOWED	2853	0xb25	Removing this entity is not allowed as entity based expression is configured
NSERR_PI_ENTITY_EXISTS	2854	0xb26	Advanced expression entity with same name already exists.
NSERR_INCOMPATIBLE_CALLOUT_CHANGE	2855	0xb27	Incompatible callout change for in-use callout.
NSERR_STRINGMAP_NOTPRESENT	2856	0xb28	String map does not exist
NSERR_HTTP_PROFILE_ACTION_NOT_ALLOWED	2857	0xb29	Responder action using HTTP protocol expressions is not allowed in HTTP profile
NSERR_RSP_ACT_MUST_BE_DROP_N	2858	0xb2A	Policy action must be DROP|NOOP|RESPONDWITH

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
OOP_RESPONDWITH			
NSERR_RSP_ACT_MUST_BE_DROP_NOOP	2899	0xb53	Policy action must be DROP|NOOP
NSERR_RSP_UNDEF_ACT_MUST_BE_DROP_NOOP	2859	0xb2B	Policy undef action must be DROP| NOOP
NSERR_INCOMPATIBLE_UNDEF	2860	0xb2C	Incompatible global undef action for SIP policy
NSERR_PIT_ACTION_EVAL_INVAL	2861	0xb2d	Action cannot be evaluated due to wrong input type.
NSERR_STRLIT_MAXLEN	2863	0xb2f	String literal length exceeds maximum. Allowed maximum length is 32767 bytes or the maximum expression length, whichever is less. In most situations the maximum expression length is either 8191 or 1499 bytes.
NSERR_DATASET_INVALID	2866	0xb32	Invalid dataset element
NSERR_DATASET_BINDFAIL_DUP_PATTERN	2867	0xb33	Pattern already bound to dataset/ patset, try using another pattern
NSERR_TIMER_ACT_INVAL	2868	0xb34	Invalid timer action

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_TIMER_ENTITY_INUSE	2869	0xb35	Timer entity name already in use
NSERR_TIMER_ENTITY_GLOBAL_BINDPOINT_INVAL	2870	0xb36	Invalid global bindpoint
NSERR_PATSET_BUILTIN	2871	0xb37	Built-in Patsets cannot be modified or deleted
NSERR_CROSS_MAX_LIMIT	2872	0xb38	Maximum value can be 2147483647
NSERR_INVALID_IPV4_FORMAT	2873	0xb39	Value should be in IPv4 format
NSERR_INVALID_IPV4_MAX_FIELD_VALUE	2880	0xb40	Maximum value of an IPv4 field can be 255
NSERR_INVALID_IPV6_FORMAT	2881	0xb41	Invalid IPv6 address format
NSERR_INVALID_NUMERIC_FORMAT	2882	0xb42	Value should be in decimal or hexadecimal format
NSERR_VALID_PREFIX_NUMERIC_FORMAT	2048	0x800	Value is valid decimal or hexadecimal format, but is only a prefix of the string
NSERR_DATASET_PATTERN_ALREADY_BOUND	2883	0xb43	Specified pattern or range is already bound to dataset/ patset

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_PI_CIRCULAR_REFERENCE_DETECTED	2884	0xb44	Circular reference detected
NSERR_INVALID_ULONG_FORMAT	2885	0xb45	Value should be in unsigned long format like 23445, 88888999
NSERR_INVALID_MAC_ADDRESS_FORMAT	2886	0xb46	Value should be in mac address format like ff:ff:ff:ff:ff:ff
NSERR_INVALID_DOUBLE_FORMAT	2887	0xb47	Value should be in double format like 223, 22.3, 234e2
NSERR_CROSS_ULONG_MAX_LIMIT	2888	0xb48	Maximum value can be 18446744073709551615
NSERR_INVAL_AVP_INSERT_EXPR	2890	0xb4a	Rewrite policy has invalid action. For Diameter bind points use DIAMETER.NEW_AVP() in action and for Radius bind points use RADIUS.NEW_AVP() in action as stringBuilderExpr expression to insert/replace AVP
NSERR_INVAL_AVP_LOOKUP_EXPR	2891	0xb4b	Rewrite policy has invalid action. For Diameter/Radius bind points, use AVP

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
			lookup expression as target expression. e.g. RADIUS.REQ.AVP(127)/ DIAMETER.REQ.AVP(9000)/ AVP_START/ AVP_END
NSERR_INVAL_DELETE_AVP_EXPR	2892	0xb4c	Rewrite policy has invalid action. Deletion of AVP should be done using AVP based expression like RADIUS.REQ.AVP(33)/ DIAMETER.REQ.AVP(9999)
NSERR_INVAL_NEW_MESSAGE_EXPR	2893	0xb4d	Responder policy has invalid action. Use expressions like DIAMETER.NEW_ANSWER/ DIAMETER_NEW_REDIRECT as target expression to create new diameter message and RADIUS.NEW_ANSWER/ RADIUS.NEW_ACCESSREJECT for RADIUS message
NSERR_INVAL_DIAMETER_REDIRECT_ACTION	2894	0xb4e	Binding Invalid Diameter action. Use DIAMETER.NEW_R

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
			EDIRECT as target expression to create new redirect message
NSERR_INVAL_DIAMETER_ACTION	2895	0xb4f	Invalid action for Diameter bind point.
NSERR_PIT_CONNECTION_ERROR	2897	0xb51	Connection error
NSERR_INVAL_SEARCH_AVP	2898	0xb52	AVP code should be a number
NSERR_DATASET_PATTERN_LIMIT_OVERFLOW	2900	0xb54	Cannot bind more than 50, 000 patterns to a patset/dataset
NSERR_INVAL_RADIUS_AVPCODE	2901	0xb55	RADIUS AVP code should be in 0-255 number range
NSERR_INVAL_RADIUS_RESPONSE	2902	0xb56	Invalid RADIUS response code
NSERR_RESP_ACT_REASON_PHRASE_REQUIRED	2903	0xb57	Please also specify a reason phrase with a user-defined HTTP status code.
NSERR_RESP_ACT_RESPONSE_CODE_REASON_PHRASE_NOT_ALLOWED	2904	0xb58	responseStatusCode and reasonPhrase options are allowed only for respondwithhtmlpage and redirect action types.
NSERR_RESP_ACT_INVALID_REDIRECT_CODE	2905	0xb59	For redirect action type the response status code must be

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
			in the range 300-399.
NSERR_RESP_ACT_INVALID_HTTP_STATUS_CODE	2906	0xb5A	Invalid HTTP status code.
NSERR_RESP_ACT_EMPTY_REASON_PHRASE_NOT_ALLOWED	2907	0xb5B	Empty reasonPhrase string not allowed.
NSERR_RSP_ACT_MUST_BE_DROP_NOOP_RESPONDWITH_RESET	2908	0xb5C	Policy action must be DROP|NOOP|RESPONDWITH|RESET
NSERR_MAX_STREAMING_PATTERN_LIMIT	2909	0xb5D	Maximum number of streaming patterns exceeded.
NSERR_RESP_UPDATE_HTMLPAGE_NOT_REFERENCED	1223	0x4c7	Responder HTML Page must be referenced in a responder action prior to update.
NSERR_PATSET_STREAMING_BINDFAIL_PATLEN_LT_WU_MINLEN	1224	0x4c8	Patterns which are < 3 or > 112 bytes in length are not allowed to be bound to the patset, if patset is being used for streaming search or in rewrite action search parameter.
NSERR_DATASET_RANGE_ERROR	2910	0xb5e	Dataset range error

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_DATASET_WARN_SUBNET_ADDR	2911	0xb5f	Starting subnet address masked using subnet mask to create new starting address
NSERR_PATSET_CONFIG_CHANGED	2915	0xb63	The patset/dataset configuration changed after the iterator was created/
NSERR_RSP_NOOP_ACTION_TYPE_NOT_ALLOWED	2916	0xb64	NOOP action type is deprecated and will be removed in the future - use NOOP action
NSERR_RSP_ACT_MUST_BE_DROP_NOOP_RESET	2917	0xb65	Policy action must be DROP|NOOP|RESET

RNAT ERRORS

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_RNAT_NAME_EXISTS	976	0x3d0	A RNAT with same name exists
NSERR_VLAN_IPV6_LL_N_ALLOW	962	0x3c2	IP address cannot be link-local address
NSERR_VLAN_INTF_BOUND_NSVLAN	963	0x3c3	Cannot unbind interface from nsvlan
NSERR_VLAN_INVALID	964	0x3c4	Incorrect vlan specified
NSERR_SYNC_VLAN_IPBOUND	965	0x3c5	Ipaddress binding/unbinding is not

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
			allowed on sync or default vlan
NSERR_VLAN_SUBNET_ALREADY_BOUND	966	0x3c6	Subnet already bound to this vlan
NSERR_UNABLE_GET_VLAN_IP	967	0x3c7	Unable to get vlan of the IPaddress
NSERR_IP_VLAN_BOUND	968	0x3c8	Ipaddress already bound to a vlan
NSERR_VLAN_UNABLE_ADD	969	0x3c9	Unable to add vlan
NSERR_DEFVLAN	970	0x3ca	Default VLAN or NSVLAN cannot be modified
NSERR_IPV6_ROUTING_BRIDGEGRP	971	0x3cb	vlan is part of a bridge group. Cannot enable routing
NSERR_VLAN_SDXMGMTVLAN_CLUSTER	972	0x3cc	Operation not permitted. vlan is SDX management vlan in a cluster
NSERR_ACL_INUSE_RNAT	973	0x3cd	This ACL is used for RNAT/NAT64/LSN/FORWARDINGSESSION. Action should be ALLOW
NSERR_RNAT_CM_TCPPROXY	974	0x3ce	TCPPROXY should be disabled for connection failover to work properly.

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_RNAT_DYN_PERM_RT	2413	0x96d	RNAT cannot be configured on DYNAMIC/ PERMANENT route
NSERR_RNAT_SRCIPPERSISTENCY_NOTSUPCLU	1218	0x4c2	RNAT SourceIPPersistency is not supported in Cluster.

SNMP ERRORS

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_INVALTHRESHOLD	3457	0xd81	Threshold value for this alarm is a percentage (1 - 100)
NSERR_WRONGTHRESHOLDS	3458	0xd82	Normal threshold must be lower than alarm threshold
NSERR_INVALID_SRCIP	3459	0xd83	Valid source IP: NSIP, SNIP, MIP. In cluster setup, valid source IP: CLIP, Striped SNIP. In non-default partition, valid source IP: SNIP
NSERR_THRESHOLD_UNSETTABLE	3460	0xd84	Threshold value cannot be set/unset for this alarm
NSERR_TIME_UNSETTABLE	3461	0xd85	Time interval cannot be set/unset for this alarm

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_WRONG_LOW_THRESHOLDS	3462	0xd86	Normal threshold must be higher than alarm threshold
NSERR_NOSNMPUSER	3463	0xd87	SNMP user doesn't exist
NSERR_WRONG_SNMPVERSION	3464	0xd88	Bind command allowed only for V3 traps
NSERR_V3TRAP_COMMUNITY	3465	0xd89	V3 traps cannot have community
NSERR_IPINUSE	3466	0xd8A	IP is used in SNMP trap configuration
NSERR_DEFAULTONLY	3467	0xd8B	Alarm not supported in non-default partition
NSERR_OWNERNODE	3468	0xd8C	Owner node not specified or invalid
NSERR_FIPS_SNMP	3469	0xd8D	Less secure SNMP configuration is not supported in FIPS mode

SPOTTED CONFIG ERRORS

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_NODECNT_EXCEED	4000	0xfa0	You cannot have more than 32 nodes in a nodegroup.
NSERR_INVAL_VAL_IN_DB	4001	0xfa1	Invalid values exist in database.

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_NODE_IDX_EXCEED	4002	0xfa2	Node index cannot exceed 31.
NSERR_INVALID_NODE	4003	0xfa3	Specified node does not exist.
NSERR_INVALID_VSVR	4004	0xfa4	Specified type of virtual server cannot be bound to the default nodegroup.
NSERR_VSVR_NOT_EXISTS	4005	0xfa5	Specified virtual server does not exist.
NSERR_VSVR_ALREADY_BOUND	4006	0xfa6	Specified virtual server is already bound to some other nodegroup.
NSERR_NOT_IN_SAME_NG	4007	0xfa7	Dependencies of the specified virtual server (such as backup virtual server) are not available in the virtual server's nodegroup.
NSERR_NG_NOT_EXISTS	4008	0xfa8	Specified nodegroup does not exist.
NSERR_NO_NODES_OR_BOUND	4009	0xfa9	Specified node is not valid or is already bound to the nodegroup.
NSERR_NO_NODES_OR_UNBOUND	4010	0xfaa	Specified node is not valid or is not bound to this nodegroup.

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_DEPENDENCIES_EXCEED	4011	0xfab	Specified virtual server has more than 1024 dependencies.
NSERR_VSVR_NOT_BOUND_OR_BOUND_TO_DIFFERENT	4012	0xfac	Specified virtual server is not bound to this nodegroup.
NSERR_HAVE_DEPENDENCIES	4013	0xfad	Specified virtual server has dependencies on other entities that are not part of the nodegroup. Remove these dependencies from the virtual server to bind the virtual server and its dependencies to the nodegroup.
NSERR_NG_CMDS_NOT_SUPPORTED_IN_STANDALONE	4014	0xfae	Nodegroup commands are supported only in a cluster setup.
NSERR_BIND_VS_FAILS_IF_NO_NODES_AND_STRICT_OR_STICKY	4015	0xfaf	You cannot bind an entity to a nodegroup that has no nodes and that has the strict/sticky option enabled.
NSERR_UNBIND_LASTNODE_FAILS_IF_BOUND_ENTITIES_AND_STRICT	4016	0xfb0	You cannot unbind the last node of a nodegroup that has entities bound to it and that has the strict option enabled.

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_SET_STRICT_FAILS_IF_NO_NODES_AND_BOUND_ENTITIES	4017	0xfb1	You cannot enable STRICT option for a nodegroup that has no nodes, but that has entities bound to it.
NSERR_RM_FAILS_IF_BOUND_ENTITIES	4018	0xfb2	Specified nodegroup cannot be removed, because it has entities bound to it.
NSERR_RM_NODE_FAILS_IF_BOUND_ENTITIES	4019	0xfb3	Specified cluster node cannot be removed, because it belongs to a nodegroup that has entities bound to it.
NSERR_RM_CLUSTER_FAILS_IF_BOUND_ENTITIES	4020	0xfb4	Specified cluster instance cannot be removed, because one of its nodegroups have entities bound to it.
NSERR_BIND_WILDCARDVIP_FAILS	4021	0xfb5	You cannot bind a wildcard vserver to a nodegroup.
NSERR_SQL_QUERY_TRUNCATED	4022	0xfb6	Too long SQL query to perform the database query.
NSERR_IDENT_ALREADY_BOUND	4023	0xfb7	Given identifier already bound.
NSERR_IDENT_NOT_BOUND_OR_BO	4024	0xfb8	Given identifier is not bound or bound to

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
UND_TO_DIFFERENT			some other nodegroup.
NSERR_IDENT_BOUND_TO_NG	4025	0xfb9	Cannot delete identifier that is bound to a nodegroup
NSERR_GSLB_NG_EXISTS	4034	0xfc2	Can not configure multiple GSLB nodegroups.
NSERR_GSLB_SITE_TYPE_NOT_LOCAL	4035	0xfc3	Can only perform this operation on a local GSLB site.
NSERR_NG_NOGSLB	4036	0xfc4	GSLB entities can not be bound to this nodegroup.
NSERR_SERVICE_BOUND_TO_NG	4037	0xfc5	Cannot delete a service bound to a nodegroup.
NSERR_GSLB_NG_NODE_COUNT	4039	0xfc7	This nodegroup must be bound to exactly ONE node
NSERR_GSLB_NG	4040	0xfc8	Only GSLB entities can be bound to this nodegroup.
NSERR_VPN_BOUND_TO_NG	4041	0xfc9	Cannot bind more than one node to a nodegroup that has vpn vservers bound
NSERR_VPN_BOUND_TO_OTHER_NG	4042	0xfca	Cannot bind vpn vserver to this nodegroup as other vpn vservers are

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
			bound to different nodegroup
NSERR_VPN_BOUND_TO_NG1	4043	0xfcb	Cannot bind vpn vserver to a nodegroup that has more than one node bound
NSERR_UNBIND_LASTNODE_FAILS_IF_VPNVSERVER_BOUND	4044	0xfcc	You cannot unbind the last node of a nodegroup that has vpn vserver bound.
NSERR_BIND_NODE_FAILS_IF_STICKY	4045	0xfcd	You cannot bind more than one node to a nodegroup that is sticky.
NSERR_UNBIND_LASTNODE_FAILS_IF_BOUND_ENTITIES_AND_STICKY	4046	0xfce	You cannot unbind the last node of a nodegroup that has entities bound to it and that has the sticky option enabled.
NSERR_SET_STRICT_FAILS_IF_STICKY	4047	0xfcf	You cannot enable STRICT option for a nodegroup that is sticky.
NSERR_25GSPEEDRESTRICT	4048	0xfd0	25G ports on this platform are restricted to speeds 25000, 10000, 1000 or AUTO only

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_NG_BIND_ENTITY_MISMATCH	4065	0xfe1	Nodegroup with state option, supports only cluster nodes binding
NSERR_NG_SET_BOUND	4066	0xfe2	Can not set nodegroup, since already bound
NSERR_NODE_ALREADY_BOUND_TO_STATENG	4067	0xfe3	Node already bound to state specific nodegroup
NSERR_NODE_BOUND_TO_STATENG	4068	0xfe4	Can not set the state of the cluster node when bound to nodegroup with state option
NSERR_NG_STRICT_DISABLED	4069	0xfe5	You can not disable STRICT option for nodegroup with state option
NSERR_NO_TRUE_POLICY	4071	0xfe7	No policy evaluated to TRUE
NSERR_BRIDGEAGE_DEPR	2749	0xabd	Argument deprecated[bridgeAge]. Use set l2param -bridgeAgeTimeout instead

SSL ERRORS

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_SSL_CERT	1536	0x600	Invalid certificate

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_SSL_PKEY	1537	0x601	Invalid private key, or PEM pass phrase required for this private key
NSERR_SSL_NOMATCH	1538	0x602	Certificate and private key do not match
NSERR_SSL_CERTTYPE	1539	0x603	Invalid certificate type
NSERR_SSL_NOCERT	1540	0x604	Certificate does not exist
NSERR_SSL_REFEXT	1541	0x605	Certificate is referenced by a CRL, OCSP responder, vserver, service, monitor, SSL profile, CA Cert Group, another certificate, or a policy expression using XML_ENCRYPT() or XML_DECRYPT()
NSERR_SSL_BIND	1542	0x606	Certificate binding does not exist
NSERR_SSL_LINK	1543	0x607	Certificate can't be linked to the same certificate
NSERR_SSL_NEED_SSLPROTO	1544	0x608	Object's protocol type is not SSL
NSERR_SSL_NOLINK	1545	0x609	Certificate does not have any CA link

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_SSL_BINDOR	1546	0x60A	Current certificate replaces the previous binding
NSERR_SSL_NOSVRCERT	1547	0x60B	Certificate is not a server/client certificate
NSERR_SSL_ISSUBMIS	1548	0x60C	Issuer certificate mismatch
NSERR_SSL_CRL	1549	0x60D	Invalid CRL
NSERR_SSL_NOCRL	1550	0x60E	CRL does not exist
NSERR_SSL_DHCOUNT	1551	0x60F	DH Refresh count should be 0 or >=500
NSERR_SSL_SESSTO	1552	0x610	Session timeout should be > 0
NSERR_SSL_ERSACOUNT	1553	0x611	eRSA Refresh count should be 0 or >=500
NSERR_SSL_DH_SIZE	1554	0x612	DH params of size greater than 4096 bits not supported
NSERR_DHPATH	1555	0x613	DH file path mandatory if DH enabled
NSERR_CERTHEADER	1556	0x614	Cert header tag mandatory if cert enabled
NSERR_SESSHEADER	1557	0x615	Sess header tag mandatory if sess enabled

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_CIPHER_PERM	1558	0x616	Default ciphers/ aliases cannot be added or removed
NSERR_SSL_ERSADISABLED	1559	0x617	Setting eRSA count when eRSA is disabled
NSERR_SSL_DHDISABLED	1560	0x618	Setting DH count when DH is disabled
NSERR_SSL_SESSDISABLED	1561	0x619	Setting session timeout when session reuse is disabled
NSERR_SSL_PKEY_SIZE	1562	0x61A	Certificate with key size greater than RSA4096 or DSA2048 bits not supported
NSERR_SSL_NOT_APPLICABLE	1563	0x61B	Option is not applicable for this type of service
NSERR_CERTDNHEADER	1564	0X61C	Cert DN tag mandatory if cert-DN enabled
NSERR_CERTISSUERHEADER	1565	0X61D	Cert issuer tag mandatory if cert-issuer enabled
NSERR_CIPHERHEADER	1566	0X61E	Cipher tag mandatory if cipher header enabled
NSERR_SSL_INTERNALERR	1567	0x61F	Internal Error

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_SSL_NOCACERT	1568	0x620	cacert does not exists
NSERR_SSL_REFRESHDIS	1569	0x621	crl refresh disabled
NSERR_SSL_SVRPORTNEEDED	1570	0x622	Server/port information is needed for enabling auto refresh
NSERR_SSL_BASEOBJNEEDED	1571	0x623	baseDN is required for enabling auto refresh
NSERR_SSL_CIPHER_REDIRECT	1572	0x624	Send Internal Cipher mismatch error page
NSERR_SSL_NODSA	1573	0x625	Loading of certificate and key of type DSA(DSS) is not supported with FIPS
NSERR_SSL_FIPSREFEXT	1574	0x626	The FIPS key is referenced by a certificate
NSERR_SSL_NOFIPSKEY	1575	0x627	No such FIPS key
NSERR_NOFIPSCARD	1576	0x628	Operation not permitted - no FIPS card present in the system
NSERR_SDXNOFIPSCARD	2256	0x8d0	Operation not permitted - Either FIPS card not present or not

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
			initialized, check SVM/Dom0.
NSERR_FIPSCARD NOTCONF	1577	0x629	Operation not permitted - FIPS card is not configured
NSERR_SSL_SSLV 2_REDIRECT	1578	0x62A	Send Internal SSL protocol mismatch error page
NSERR_SSL_MOD SIZE64	1579	0x62B	Modulus size in bytes should be multiple of 64
NSERR_SSL_NONF IPSKEY	1580	0x62C	Configuration of non-FIPS key on FIPS system not allowed
NSERR_NFIPS_FIP S_UPD	1581	0x62D	Cannot update a non-FIPS certificate with a FIPS certificate
NSERR_FIPS_NFIP S_UPD	1582	0x62E	Cannot update a FIPS certificate with a non-FIPS certificate
NSERR_SSL_ISSU ER_NOTIN_GLBCE RTLIST	1583	0x62F	Unable to find the CA certificate for the CRL
NSERR_SSL_CRLSI GCHECK_FAIL	1584	0x630	Signature check on the CRL failed
NSERR_SSL_PORT REWRITE	1585	0x631	SSL port rewrite can be enabled only when SSL redirect is enabled

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_SSL_SSLV2_RENEG_CLIENT_CERT	1586	0x632	Send Internal error page for SSLv2 protocol and client authentication with session renegotiation
NSERR_SSL_BRKLINK	1587	0x633	All incompatible CA links/Cert bindings were broken during the update operation
NSERR_SSL_CERT_NOT_YET_VALID	1588	0x634	The specified certificate is not yet valid
NSERR_SSL_CERT_EXPIRED	1589	0x635	The certificate has expired
NSERR_SSL_EXPIRED_BRKLINK	1590	0x636	All incompatible CA links were broken during the update operation. (Note: the certificate has expired)
NSERR_SSL_NYVALID_BRKLINK	1591	0x637	All incompatible CA links were broken during the update operation. (Note: the certificate is not yet valid)
NSERR_SSL_OCSP_RESPCERT	1592	0x638	No such responder certificate.
NSERR_SSL_OCSP_SIGNCERT	1593	0x639	No such signing certificate.
NSERR_SSL_NO_SESS_TKT	1594	0x63A	Session Ticket feature is not

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
			supported on FIPS platform
NSERR_SSL_OCSP_INVALID_AIA	1595	0x63B	Invalid OCSP AIA URL found
NSERR_SSL_OCSP_AIA_LEN_NOT_SUPPORTED	1596	0x63C	OCSP AIA URL length should be less than 126
NSERR_SSL_SSL3_SUPPORT	1597	0x63D	Enabling of SSLv3 is not supported on this platform.
NSERR_SSL_BOUNDTO_SSLACTION	1598	0x63E	Vserver cannot be removed as it's referenced by one or more SSL Actions. Remove SSL action(s) prior to removing vserver.
NSERR_SSL_INVALID_SESS_TKT_DATA	1599	0x63F	invalid session ticket key data len, length should be 64 bytes
NSERR_SSL_SAME_VS_IN_FORWARD	1600	0x640	Vserver to which packets will be forwarded cannot be same as the vserver to which this policy is getting bound.
NSERR_NAME_ALPHANUM_DASH_DOT	3358	0xd1e	Name must begin with a letter followed by letters, digits, dots or forward slash.
NSERR_SSL_PROFILE_SSLI_NOT_ALLOWED	3370	0xd2a	SSL interception can only be enabled on

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
			profile bound to proxy vserver
NSERR_SSL_CTX_SSLI_PROFILE_NOT_ALLOWED	3371	0xd2b	Profile with SSL interception enabled cannot be set on non PROXY type of vservers.
NSERR_SSL_PROFILE_SSLI_CLUSTER_NOT_SUPPORTED	3372	0xd2c	SSL interception is not supported on cluster
NSERR_SSL_DEFAULT_PROFILE_SSLI_NOT_SUPPORTED	3373	0xd2d	SSL interception cannot be enabled on default frontend SSL profile
NSERR_SSL_CERT_BOUND_TO_AAA_FEATURE	3374	0xd2e	SSL certificate is used for encrypting user data and can not be updated
NSERR_SSL_CERT_BOUND_TO_ADFSPROXY_PROFILE	3375	0xd2f	SSL certificate is bound to a adfsproxy profile and cannot be updated
NSERR_SSL_CERT_LINK_NOT_ALLOWED	3418	0xd5a	SSL certificate link can be done only for Non CA certificates
NSERR_SSL_DTLS12_SUPPORT	3391	0xd3f	DTLSv1.2 is not supported on this entity/platform.
NSERR_SSL_ERR_HTTPS_ONLY	3419	0xd5b	Invalid Protocol. Only HTTPS supported.

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_SSL_PROFILE_SSLI_ADMIN_PARTITION_NOT_ALLOWED	3420	0xd5c	SSL interception is not supported in non-default partition
NSERR_SSL_INVALID_CA_BASIC_CONSTRAINT	3422	0xd5e	CA Certificate does not have the required Basic constraints extensions

SSL2 ERRORS

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_SSL_FIPSCARDLOCKED	3584	0xe00	FIPS card locked due to three unsuccessful login attempts
NSERR_SSL_DOMINCOMPAT	3585	0xe01	Certificate is registered to a different domain; use the 'no domain check' option to force the operation
NSERR_SSL_NOMTHDCHANGE	3586	0xe02	Cannot change refresh method of CRL
NSERR_SSL_URLSRVRNEEDED	3587	0xe03	Either URL or server-IP required on CRL
NSERR_SSL_INVALID_URL	3588	0xe04	Invalid URL
NSERR_SSL_MIXPARAMS	3589	0xe05	LDAP and HTTP parameters cannot both be specified

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_SSL_PKEY_MINSIZE	3590	0xe06	Certificate of size smaller than 512 bits not supported
NSERR_SSL_SYNCINPROGRESS	3591	0xe07	Another synchronization is already in process, please try again later
NSERR_SSL_SYNCFAILED	3592	0xe08	Synchronization failed, please try again
NSERR_SSL_CIPHGRP_REFCNT	3593	0xe09	Cipher group has bound entities or is referenced by an SSL vserver or SSL service
NSERR_SSL_CVM_NODSA	3594	0xe0A	Loading DSA(DSS) certificate and key not supported on this platform
NSERR_CERTHASHHEADER	3595	0xe0B	CertHash header tag mandatory if certHash is enabled
NSERR_SSL_CRLINREFRESH	3596	0xe0C	CRL refresh in progress, details cannot be displayed
NSERR_SSL_CRLMEM_EXCEEDS	3597	0xe0D	CRL memory exhausted. Cannot load any more CRL's
NSERR_SSL_CRLINDELETION	3598	0xe0E	CRL deletion in progress, details cannot be displayed

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_SSL_INDELETE_NOREFRESH	3599	0xe0F	CRL deletion in progress, cannot be refreshed
NSERR_SSL_INREFRESH_NODELETE	3600	0xe10	CRL refresh in progress, cannot be removed
NSERR_NOMIX	3601	0xe11	Cannot specify both HTTP data insertion and SSL actions
NSERR_SSL_NONSSL_SERVICE	3602	0xe12	SSL policy binding is not supported for this service
NSERR_SSL_SSLPOL_BIND_CONST	3603	0xe13	Cannot bind non-SSL policy to SSL vserver/service
NSERR_SSL_NO_USABLE_CIPHERS	3604	0xe14	No usable ciphers configured on the SSL vserver/service
NSERR_SSL_CERT_NOT_CA	3605	0xe15	Not a CA certificate
NSERR_SSL_CACERT_NO_CRLSIGN	3606	0xe16	Specified certificate is either not a CA cert, or does not have privileges to issue CRLs
NSERR_SSL_CRL_EXPIRED	3607	0xe17	CRL has expired
NSERR_SSL_CRL_NOTYET_VALID	3608	0xe18	CRL is not yet valid

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_SSL_PARSING_DELTA_CRL_EXTN	3609	0xe19	Parsing of Delta-CRL extension failed
NSERR_SSL_DELTA_CRL_MISSING_BASE_CRL	3610	0xe1A	Base-CRL for the specified Delta-CRL is missing
NSERR_NOFIPSCIPHER	3611	0xe1B	Specified cipher/ cipher-alias is not FIPS-approved
NSERR_NOFIPSCIPHERGRP	3612	0xe1C	Cipher group does not contain all FIPS-approved ciphers
NSERR_NONFIPSCIPHERTOGRP	3613	0xe1D	Cannot add non FIPS approved cipher to cipher group
NSERR_NONFIPSALIASTOGRP	3614	0xe1E	Cannot add non FIPS approved cipher alias to cipher group
NSERR_NONFIPSGROUPTOGRP	3615	0xe1F	Cannot add non FIPS cipher group to another cipher group
NSERR_SSL_IMPORT_FIPSKEY_NAME_MISMATCH	3616	0xe20	Specified FIPS key name does not match with the exported FIPS key name
NSERR_SSL_PKEY_SIZE_CA	3617	0xe21	CA certificate of size greater than 4096 bits not supported

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_SSL_CRL_PORT_MISMATCH	3618	0xe22	Port specified in URL does not match -port parameter
NSERR_SSL_PKEY_SIZE_VPX	3619	0xe23	Certificate with key size greater than RSA512 or DSA512 bits not supported
NSERR_SSL_DH_SIZE_VPX	3620	0xe24	DH params of size greater than 512 bits not supported
NSERR_NOENT_CIPHER	3621	0xe25	No such cipher/ cipherAlias/ cipherGroup
NSERR_FIPSFWWRONGMAJOR	3622	0xe26	The current firmware's major version is not supported for update operation
NSERR_FIPSFWWRONGMINOR	3623	0xe27	The current firmware's minor version is not supported for update operation
NSERR_FIPSFWUPDATED	3624	0xe28	The current firmware is already updated to 4.6.1
NSERR_SSL_PENDING_CMDS	3625	0xe29	Other commands (card health monitoring/traffic) are pending to FIPS card. Please try the firmware update

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
			command after some time
NSERR_FIPSFWUPDATEDOREBOOT	3626	0xe2A	Operation not permitted - FIPS card firmware update done, please reboot the system
NSERR_SSL_SNI_NOTENABLE	3627	0xe2B	SNI feature not enabled on the vserver/service
NSERR_SSL_NO_CN	3628	0xe2C	CommonName not present in certificate, it is must for a certificate to use for SNI
NSERR_SSL_DUP_SNICERT	3629	0xe2D	Trying to bind SNI certificate with duplicate CommonName, operation failed
NSERR_SSL_SNI_NOTVALID_SERV	3630	0xe2E	Operation not permitted - SNI feature not supported on internal service or DTLS backend services
NSERR_SSL_NOT_SUPPORTED_ON_PLATFORM	3631	0xe2F	Feature not supported on this platform
NSERR_OCSP_REFERENCES	3632	0xe30	OCSP responder is bound to a vserver/certkey pair. Use unbind ssl certkey.

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_OCSP_SIGNER_NOKEY	3633	0xe31	Signing certificate must also have a private key.
NSERR_SSL_NOT_SUPPORTED	3634	0xe32	OCSP responder must be an HTTP server; SSL is not supported.
NSERR_OCSP_TOO_MANY_RESPONDERS	3635	0xe33	Too many OCSP responders configured to add another. Please delete some and try again.
NSERR_OCSP_NO_DNS_SERVER_CONFIGURED	3636	0xe34	Unable to resolve DNS name.
NSERR_SSL_DUP_SNICERT_BRKLINK	3637	0xe35	Some of the existing SNI cert bindings are broken due to presence of certificate with duplicate Common Name.
NSERR_SSL_NO_CN_BRLLINK	3638	0xe36	All existing SNI Cert bindings are broken during update operation due to missing Common Name.
NSERR_NGFIPSRESETREBOOT	3639	0xe37	Operation not permitted - FIPS card was reset, please reboot the system

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_NGFIPSINITREBOOT	3640	0xe38	Operation not permitted - FIPS card was initialized, please reboot the system
NSERR_FIPSCMDTIMEOUT	3641	0xe39	Operation timed out on the FIPS card, please try again
NSERR_SSL_SIMTIMEOUT	3642	0xe3a	Operation timed out or repeated, please wait for 10 mins and redo the SIM/HA configuration steps.
NSERR_SSL_NGFIPS_QFULL	3643	0xe3b	FIPS card command queue full. Please try again later
NSERR_SSL_NOMEM_VSVRSRVLISTNODE	3644	0xe3c	Failed to allocate memory for CertkeyVserverServ List Node.
NSERR_SSL_CERTKEY_SIZE64	3645	0xe3d	Certificate with key size (modulus) that is not multiple of 512 bits is not supported
NSERR_SNI_ATK	3646	0xe3e	Host header field in the HTTP request does not match with the SNI domain name
NSERR_SNI_NOHOSTHDR	3647	0xe3f	Host header missing in the HTTP header for SNI enabled session

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_CRL_SHMEM_ALLOC_FAIL	3648	0xe40	Crl node allocation in the shared mem is failed
NSERR_SSL_NOT_CTL_POL	3650	0xe42	Not a control policy
NSERR_SSL_NOT_DATA_POL	3651	0xe43	Not a data policy
NSERR_SSL_TYPE_REQD	3652	0xe44	Type is required
NSERR_SSL_CERT_MISSING_PARAM	3655	0xe47	Required parameters missing in the certificate. Please check the certificate for completeness
NSERR_SSL_NOMEM_CERTKEY_OCSPRESP_LISTNODE	3656	0xe48	Failed to allocate memory for CertkeyOCSPRespList Node.
NSERR_SSL_OCSP_DUPLICATE	3657	0xe49	An ocspResponder is already bound with the specified priority.
NSERR_SSL_BUNDLE_IC_FILE_EXISTS	3660	0xe4c	Certificate file for intermediate certificate already exists.
NSERR_SSL_BUNDLE_SCERT_MISSING	3661	0xe4d	Server certificate must be placed first in certificate bundle file.

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_SSL_BUNDLE_CERT_MISSING	3662	0xe4e	No certificates present in the certificate bundle file.
NSERR_SSL_BUNDLE_FAILED	3663	0xe4f	Processing of certificate bundle file failed.
NSERR_SSL_BUNDLE_PARSE_ERR	3664	0xe50	Unable to parse the certificate bundle file.
NSERR_SSL_BUNDLE_MAX_CERT	3665	0xe51	Exceeded maximum Intermediate certificates limit of 9.
NSERR_SSL_BUNDLE_MAX_KEY	3666	0xe52	Only one private-key is allowed in the certificate bundle file.
NSERR_SSL_BUNDLE_IC_FILE_CREATE_FAILED	3667	0xe53	Intermediate certificate file creation failed.
NSERR_SSL_SKIPCA_OPNOTPER	3668	0xe54	skipCA is not permitted for this entity.
NSERR_SSL_ISSUER_MISMATCH	3669	0xe55	Certificate Issuer mismatch
NSERR_SSL_SET_POLICY_ACTION_TYPE	3670	0xe56	Action type cannot be changed from the previous configured action type
NSERR_SSL_DTLS_NOTSUPP	3671	0xe57	Server/Service of type DTLS is not supported on this platform

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_SSL_INVALID_CN_NAME	3672	0xe58	Invalid Common Name.
NSERR_SSL_ECC_NOT_SUPPORTED	3673	0xe59	ECDHE ciphers supported only on FE SSL entities on VPX, MPX and BE MPX
NSERR_SSL_NO_PROTOCOL_ENABLED	3674	0xe5a	SSL or TLS protocols not enabled on the service.
NSERR_SSL_SSL2_NOT_SUPPORTED	3675	0xe5b	SSLv2 not supported in this release
NSERR_DTLS_PROFILE_REFEXT	3676	0xe5c	DTLS profile is referenced by a vserver or front-end service.
NSERR_SSL_NO_ECC_CURVES	3677	0xe5d	No ECC curves bound for ECDHE ciphers.
NSERR_CRYPTODEV_MAX_LIMIT	3678	0xe5e	Crypto Device count exceeds maximum available.
NSERR_SSL_PROFILE_ATTACHED	3679	0xe5f	Operation not permitted. Use set ssl profile for setting these parameters.
NSERR_SSL_PROFILE_USED	3680	0xe60	Profile is being used by Virtual Server, Service or Monitor.

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_SSL_PROFILE_NOT_VAILD_PARAM	3681	0xe61	Specified parameters are not applicable for this type of SSL profile.
NSERR_IMPORT_SSL_INVALID_DHFILE_ERROR_OBJECT	3682	0xe62	Import failed: DH file being imported is invalid.
NSERR_IMPORT_SSL_INVALID_CRLFILE_ERROR_OBJECT	3683	0xe63	Import failed: CRL file being imported is invalid.
NSERR_IMPORT_SSL_INVALID_CERTFILE_ERROR_OBJECT	3684	0xe64	Import failed: Certificate file being imported is invalid
NSERR_IMPORT_SSL_INVALID_KEYFILE_ERROR_OBJECT	3685	0xe65	Import failed: Key file being imported is invalid
NSERR_FIPSFW_FILEPATH	3686	0xe66	Invalid firmware file path
NSERR_FIPSFW_FILEOPEN	3687	0xe67	Unable to open firmware file
NSERR_FIPSFW_FILEIO	3688	0xe68	Read error occurred for firmware file
NSERR_FIPSFW_FSTAT	3689	0xe69	Failed to get status of firmware file
NSERR_FIPSFW_AUTH_FILEPATH	3690	0xe6a	Invalid firmware signature file path

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_FIPSFW_AUTH_FILEOPEN	3691	0xe6b	Unable to open firmware signature file
NSERR_FIPSFW_AUTH_FILEIO	3692	0xe6c	Read error occurred for firmware signature file
NSERR_FIPSFW_AUTH_FSTAT	3693	0xe6d	Failed to get status of firmware signature file
NSERR_FIPSFW_BEGIN_ERROR	3694	0xe6e	Firmware update process failed BEGIN command
NSERR_FIPSFW_UPDATE_ERROR	3695	0xe6f	Firmware update process failed UPDATE command
NSERR_FIPSFW_END_ERROR	3696	0xe70	Firmware update process failed END command
NSERR_FIPSFW_STATE_ERROR	3697	0xe71	Firmware update process failed, invalid state
NSERR_FIPSFW_INVALID_CHUNK_TYPE	3698	0xe72	Firmware update process failed, invalid chunk type
NSERR_SSL_OCSP_WITH_CK_HSMKEY	3699	0xe73	Configuration of OCSP signing certificate with external HSM key not supported.
NSERR_SSL_HSMKEY_DEFLOCATION	3700	0xe74	Input HSM Key Simple file does not present under the

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
			default directory /var/opt/nfast/kmdata/local/
NSERR_SSL_HSMKEY_IDENT_MISMATCH	3701	0xe75	HSM Key Name must be same as HSM Key Ident
NSERR_SSL_HSMKEY_DTLS	3702	0xe76	HSM Key bind with DTLS Vserver is not supported.
NSERR_SSL_HSMKEY_BUNDLE	3703	0xe77	Addition of certificate-bundle with external HSM Key is not supported.
NSERR_CPE_EXPRESSION_PARTITION_INVALID	3704	0xe78	Classic expression is not supported in current partition.
NSERR_AP_INVALID_EXPRESSION	3705	0xe79	Expression value not supported.
NSERR_SSL_DH_BUSY	3706	0xe7a	DH Param in use. Please try later...
NSERR_FIPSFW22_MINKEYSIZE	3707	0xe7b	Key size less than 2048 is not supported on FIPS Firmware Version 2.2.
NSERR_SSL_MAXSAN	3708	0xe7c	Maximum number of SANs reached
NSERR_SSL_BADSNICERT	3709	0xe7d	Bad SNI certificate

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_SSL_AESGCM_SHA2_NOT_SUPPORTED	3710	0xe7e	SHA2 ciphers not supported on VPX and FIPS
NSERR_SSL_NOCIPHERGRP	3711	0xe7f	Cipher Group does not exist.
NSERR_SSL_SVCVSR_NOT_FOUND	3712	0xe80	No SSL vserver/ service found with this name.
NSERR_SSL_DEF_DTLS_PROFILE	3713	0xe81	Cannot modify default DTLS profile.
NSERR_SSL_NOSSLV2REDIRECTOPT_ON_FIPS	3714	0xe82	Sslv2 Redirect option is not permitted on MPX-FIPS platform.
NSERR_SSL_OP_ON_NONFIPS_NOT_PERM	3715	0xe83	Operation permitted only on MPX-FIPS platform.
NSERR_SSL_LOAD_KEYS	3716	0xe84	Loading of internal keys failed.
NSERR_SSL_PASSWORD_DECODE	3717	0xe85	Decode of the encrypted passphrase failed.
NSERR_SSL_NOCERT_FILE	3718	0xe86	Certificate file name not specified.
NSERR_SSL_DEFAULT_CERT_DEL	3719	0xe87	Cannot delete internal default certificate.
NSERR_SSL_FIPS_CERT	3720	0xe88	FIPS certificate cannot be bound as a CA certificate,

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
			install the certificate without the FIPS key.
NSERR_SSL_CERTKEY_HSM	3721	0xe89	Cannot bind a certificate with HSM key to a service.
NSERR_SSL_DEFAULT_CERT_BIND	3722	0xe8a	Cannot bind internal default certificate.
NSERR_SSL_CMD_DEPRECATED	3723	0xe8b	Command deprecated, operation not applicable to this platform.
NSERR_SSL_NO_LIC	3724	0xe8c	Only export ciphers are allowed without proper SSL license.
NSERR_SSL_DTLS_NA	3725	0xe8d	Command arguments does not apply to vserver/ service of type DTLS.
NSERR_SSL_ECC_SUPPORT	3726	0xe8e	ECC curve is not supported for this entity/platform.
NSERR_SSL_PROFILE_FE	3727	0xe8f	Cannot bind front-end profile to a back-end SSL service.
NSERR_SSL_PROFILE_BE	3728	0xe90	Cannot bind back-end profile to a front-end SSL vserver.
NSERR_SSL_OP_ON_FIPS_WOFW22_NOT_PERM	3729	0xe91	Operation not permitted on MPX-FIPS platform

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
			without FIPS firmware version 2.2 or higher.
NSERR_SSL_NONSSL_VSERVER	3730	0xe92	Vserver is not of type SSL/HTTP_QUIC.
NSERR_SSL_UDP_DTLS	3731	0xe93	Cannot bind policy to vserver of type DTLS.
NSERR_SSL_TLS11_12_SUPPORT	3732	0xe94	Enabling of TLSv1.1/1.2 is not supported on this entity/platform.
NSERR_SSL_HSM_KEY_SVC_SVCGRP	3733	0xe95	Binding of certificate with HSM key is not supported on back-end service, serviceGroup or monitors.
NSERR_DTLS_PROFILE	3734	0xe96	Cannot bind DTLS profile to an SSL vserver.
NSERR_SSL_PROFILE_NO_USABLE_CIPHERS	3735	0xe97	No usable ciphers configured for some of the SSL vserver/ service bound to this profile
NSERR_SSL_CIPHGRP_NO_USABLE_CIPHERS	3736	0xe98	No usable ciphers configured for some of the SSL vserver/ service bound to this cipher group

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_SSL_PROFILE_UNSET_DEFAULT	3737	0xe99	Unsetting a default SSL Profile is not allowed
NSERR_SSL_DEFAULT_PROFILE_ENABLED	3738	0xe9a	Disabling ssl default profile is not allowed
NSERR_SSL_PROFILE_DEFAULT_DISABLED	3739	0xe9b	Operation not permitted. To do this Enable default ssl profile by setting 'set ssl parameter -defaultProfile E'
NSERR_SSL_PROFILE_DEFAULT_ENABLED	3740	0xe9c	Operation not permitted. Use profile command to do this operation
NSERR_SSL_CIPHER_EXIST_HIGHER_PRI	3741	0xe9d	Specified cipher is already bound with higher priority
NSERR_SSL_DEFAULT_PROFILE_PERM	3742	0xe9e	Default ssl profile can not be removed
NSERR_SSL_DH_SIZE_16B	3743	0xe9f	DH params of size is not 16B aligned
NSERR_SSL_NOCIPHERREDIRECTOPT	3744	0xea0	The cipher redirect option is not supported for SSL Service
NSERR_SSL_NOCLIENTAUTHOPT	3745	0xea1	The client auth option is not supported for SSL Service

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_SSL_NOSSLV2REDIRECTOPT	3746	0xea2	The SSLv2 redirect option is not supported for SSL Service
NSERR_SSL_NONONFIPSCIPHERSOPT	3747	0xea3	The nonFipsCiphers option is not applicable anymore
NSERR_SSL_NOCIPHERREDIRECTOPT_ON_FIPS	3748	0xea4	Cipher Redirect option is not permitted on MPX-FIPS platform.
NSERR_SSL_NOSSL2PROTOOPT_ON_FIPS	3749	0xea5	Ssl2 protocol option is not permitted on MPX-FIPS platform.
NSERR_SSL_CANNOT_BIND_VSERVER	3750	0xea6	Front end service cannot be bound to a vserver.
NSERR_SSL_SERVERAUTHNOTSUPP	3751	0xea7	ServerAuth Operation is not supported for front end service.
NSERR_SSL_SERVERAUTH_SNI_REQUIRED	3752	0xea8	Argument pre-requisite missing serverAuth == ENABLED or SNIEnable == ENABLED
NSERR_SSL_CN_REQUIRED	3753	0xea9	Argument pre-requisite missing commonName
NSERR_SSL_DTLSPROFNOTSUPP	3754	0xeaa	DTLS options are not applicable to non-

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
			DTLS vserver/ Service
NSERR_SSL_PUSHENCNOTSUPP	3755	0xeab	Push encryption trigger is not supported for SSL Service.
NSERR_N3FIPS_MINKEYSIZE	3756	0xeac	Key size less than 2048 is not supported on N3FIPS
NSERR_N3FIPS_MAXKEYSIZE	3757	0xead	Key size more than 3072 is not supported on N3FIPS
NSERR_N3FIPS_MINEXPSIZE	3758	0xeae	N3FIPS only supports F4(65537) as an exponent
NSERR_SSL_OCSPNAMENOTSUPP	3759	0xeaf	OCSP responder name should not start with ns_internal/ ns_zt_static_resp/ ns_zt_dynamic_resp.
NSERR_SSL_OCSP_NOT_VALID_PARAM	3760	0xeb0	Specified parameters are not applicable for this type of ocsp responder.
NSERR_SSL_NOOCSPSTAP	3761	0xeb1	Ocsp stapling option is not supported for SSL Service.
NSERR_SSL_CREATE_AIA_OCSP_RESP_FAILED	3762	0xeb2	Failed to create/bind Internal Ocsp responder(using certkey AIA URL).

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_N3FIPDEXUPGRADE	3763	0xeb3	N3FIPS VPX does not support upgrade firmware operation
NSERR_N3FIP_MAXKEYNUM	3764	0xeb4	Maximum Fips keys limit reached
NSERR_FIPSCARDCONFIGED	3765	0xeb5	Fips is already configured, please reset first to set fips again
NSERR_N3FIPSCHANGELIC	3770	0xeba	N3FIPS license is changed, please reboot the system
NSERR_SSL_OCSP_SET_NOT_ALLOWED_ON_AIA	3771	0xebb	Set operation on internal ocsp entity is not allowed
NSERR_SSL_TLS13_SUPPORT	3775	0xebf	Enabling of TLSv1.3 is not supported on this entity/platform.
NSERR_SSL_CLEARTEXTPORT_WARNING	3778	0xec2	Cannot set cleartextport for a ssl service.
NSERR_SSL_DH_SIZE_2048	3780	0xec4	DH params of size greater than 2048 bits not supported on this platform.
NSERR_SSL_DEFAULT_CERT_NAME	3802	0xeda	Cannot use this name in non-default partition.
NSERR_SSL_VS_NOT_ALLOWED	3803	0xedb	Vserver should be of type: TCP,

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
			SSL_BRIDGE, SSL_TCP or SSL.
NSERR_SSL_CACERTGROUP_EXIST	3566	0xdee	CA certificate group already exists.
NSERR_SSL_CACERTGROUP_NOTEXIST	3567	0xdef	CA certificate group does not exist.
NSERR_SSL_CACERTGROUP_REF	3579	0xdfb	Certificate group is referenced by SSL action(s).
NSERR_SSL_NOT_CACERT	3580	0xdfc	Certificate is not a CA certificate.
NSERR_SSL_GROUP_HAS_CACERTKEY	3581	0xdfd	CA certificate group already has an entry for this CA certificate-key.
NSERR_SSL_GROUP_HAS_NO_CACERTKEY	3583	0xdff	CA certificate group does not have an entry for this CA certificate-key.
NSERR_SSL_SNICERT_INVALID	3805	0xedd	Cannot bind SNI cert on an internal and backend service. SNI cert can be bound only to SSL vserver.
NSERR_SSL_NO_CERTKEY_FILE	3807	0xedf	CertKey files deleted from file system, do save config, unsaved reboot will not bring deleted certKey files.
NSERR_SSL_NO_PRIVATE_KEY	3827	0xef3	Private Key is not present.

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_SSL_NO_DTLS_PROTOCOL_ENABLED	1691	0x69b	DTLS protocols not enabled on the vserver/service.
NSERR_SSL_PROFILE_QUIC_MISMATCH	1776	0x6f0	SSL profiles of type QUIC-FrontEnd/ QUIC-BackEnd can only be associated with HTTP_QUIC virtual servers/ services.
NSERR_SSL_DH_SIZE_INTEL_CRYPTO	1777	0x6f1	DH params key size is not supported in the Intel Crypto platform, supported key sizes 768, 1024, 1536, 2048, 3072, 4096.
NSERR_SSL_CONVERT_TO_DEFAULT PROFILE_FAILED	1778	0x6f2	Conversion to Default Profile Failed
NSERR_SSL_VAULT_NOT_EXIST	1779	0x6f3	Vault does not exist
NSERR_SSL_CERT_NOT_FROM_VAULT	1780	0x6f4	Certificate is not fetched from the vault.
NSERR_SSL_VAULT_BIND_DTLS_VPN	1781	0x6f5	Vault bind and unbind is not supported with DTLS v-server ; VPN v-server with DTLS on.
NSERR_SSL_VAULT_NO_AZURE_APP	1782	0x6f6	Azure application is not found.

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_SSL_VAULT_UNBIND_FIRST	1783	0x6f7	Unbind existing Vault first, then bind a new vault to the v-server.
NSERR_SSL_PROFILE_ENABLE_EMS	1784	0x6f8	If using versions below TLS1.2, disallowing legacy KDF will prevent connections. If using TLS1.2, please make sure to set '-allowExtendedMasterSecret YES' in the profile to continue handling connections.

SSLVPN AAA ERRORS

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_ERR_AAA_LICENSE	2624	0xa40	MaxAAAUsers value more than allowed by license, ignored.
NSERR_USR_NOINTRAIP	2625	0xa41	No intranet IP bound to user
NSERR_USR_NOTCONFIGURED	2626	0xa42	User does not exist
NSERR_INVAL_AAA_GRP	2627	0xa43	Group does not exist
NSERR_INVAL_COMBNATION	2628	0xa44	NONE and ALL cannot be used simultaneously

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_INVAL_MIP_IIP	2629	0xa45	Both Mapped IP and Intranet IP must be specified
NSERR_INVAL_MIPOFF_IIPOFF	2630	0xa46	Mapped IP and Intranet IP cannot be OFF at the same time
NSERR_USEREXIST	2631	0xa47	User already exists
NSERR_GROUPEXIST	2632	0xa48	Group already exists
NSERR_USERALREADYBOUND	2633	0xa49	User is already bound to the group
NSERR_NO_RADIUS_IP	2634	0xa4a	ServerIP is not configured in radius params
NSERR_NO_TACACS_IP	2635	0xa4b	ServerIP is not configured in tacacs params
NSERR_USERNOTBOUND	2640	0xa50	User is not bound to the group
NSERR_ENTITYNOTBOUND	2641	0xa51	Entity not bound
NSERR_GROUPNOTEXIST	2642	0xa52	Group does not exist
NSERR_INVALIDLOGLEVEL	2643	0xa53	NONE cannot be combined with other options

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_DH_MISCONFIG	2644	0xa54	The first hop and second hop can not be enabled on the same vserver
NSERR_DH_IPPORT	2645	0xa55	The SG second hop ip and port are required
NSERR_DHINUSE	2646	0xa56	Bound double hop server cannot be removed
NSERR_INVAL_AAAGLOBAL_POLTYPE	2647	0xa57	Only preauthentication policies can be bound to AAA global
NSERR_NO_LDAP_IP	2648	0xa58	ServerIP is not configured in ldap params
NSERR_AAATM_LIC	2649	0xa59	Feature not licensed [AAA]
NSERR_AAATM_DISABLED	2650	0xa5a	Feature(s) not enabled [AAA]
NSERR_NO_AUTH_HOST	2651	0xa5b	No Authentication Host specified
NSERR_AUTH_ON	2652	0xa5c	Turn authentication off first
NSERR_KILLPENDING	2653	0xa5d	Another kill command in progress
NSERR_AAATM_NO_AUTH_VS	2654	0xa5e	No Authentication vserver name

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
			specified or the server does not exist
NSERR_AAATM_401AUTH_ON	2655	0xa5f	Turn off 401 based authentication first
NSERR_UNAUTHRZED	2656	0xa60	Unauthorized
NSERR_KILL_INPROGRESS	2657	0xa61	A kill session command is in progress. Try again later
NSERR_WI_FRM_NOTEXIST	2658	0xa62	Farm does not exist
NSERR_WI_FRM_LAST	2659	0xa63	At least one Farm should be configured: can not remove last farm
NSERR_WI_NOTINST	2660	0xa64	Web interface not installed
NSERR_WI_GENFAILED	2661	0xa65	Unable to generate website
NSERR_WI_SITE_EXIST	2662	0xa66	Site already exists
NSERR_WI_SITE_NOTEXIST	2663	0xa67	Site does not exist
NSERR_WI_SITE_INVAL_AGURL	2664	0xa68	Invalid agURL
NSERR_WI_SITE_INVAL_STAURL	2665	0xa69	Invalid staURL

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_WI_SITE_ONLY_MPX	2666	0xa6a	WI can only be installed on NetScaler nCore builds
NSERR_WI_INSTFAILED	2667	0xa6b	Installation failed. Please check the log file /var/log/wicmd.log
NSERR_WI_MAXSITE_EXCD	2668	0xa6c	Maximum number of WI Sites exceeded. Please check the log file /var/log/wicmd.log
NSERR_WI_STAWITHOUTAGURL	2669	0xa6d	STAUrl cannot be specified without AGUrl.
NSERR_WI_AGURLWITHOUTSTA	2670	0xa6e	AGUrl cannot be specified without STAUrl.
NSERR_WI_RELWITHOUTAGURL	2671	0xa6f	SessionReliability cannot be ON without AGUrl.
NSERR_WI_AUTHWITHOUTAGURL	2672	0xa70	AuthenticationPoint cannot be specified without AGUrl.
NSERR_WI_TWOKTWITHOUTREL	2673	0xa71	UseTwoTickets cannot be ON without SessionReliability.
NSERR_WI_TWOKTWITHOUTSECSTA	2674	0xa72	UseTwoTickets cannot be ON

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
			without SecondSTAUrl.
NSERR_WI_SECSTASAME	2675	0xa73	SecondSTAUrl should be different from StaURL.
NSERR_WI_LICENSE	2676	0xa74	Web Interface on NS Feature not licensed.
NSERR_WI_SECSTAWITHOUTSTA	2677	0xa75	SecondSTAUrl cannot be specified without STAUrl.
NSERR_AUTH_NEGOTIATE	2678	0xa76	Negotiate authentication required
NSERR_WI_INSTSITESREDUCED	2679	0xa77	Memory available is not sufficient for the passed maxSites value
NSERR_WI_INCOMPATIBLEAUTHPOINT	2680	0xa78	WI Authentication methods can not be specified unless authentication point is WI
NSERR_WI_SITE_WITHIN_SITE	2681	0xa79	One WI site can not be completely within another WI site
NSERR_WI_SITE_TRANSLATION_NOEXIST	2682	0xa7a	Translation Map does not exist
NSERR_WI_SITE_TRANSLATION_LAST	2683	0xa7b	Can't Unbind Last Translation Map

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_WI_SITE_NOAGURL	2684	0xa7c	AGURL is not set
NSERR_AGSVC_AUTHFAIL	2685	0xa7d	AG-Service request with invalid AAAC cookie
NSERR_TM_INVALID_PERS_CONFIG	2686	0xa7e	Please specify both persistentCookie and persistentCookieValidity parameters
NSERR_WI_SMARTCARD_NOT_SUPPORTED	2687	0xa7f	SmartCard AGAuthentication method is not supported with sites created using wi package
NSERR_WI_SEARCH_NOT_SITEWEB	2688	0xa80	Show Search Attribute supported only for site type XenAppWeb
NSERR_KCD_ACCOUNT_NOT_EXISTS	2689	0xa81	The KCD account does not exist
NSERR_KCD_KEYTAB_NOT_EXISTS	2690	0xa82	The keytab file does not exist
NSERR_KCD_VS_PRINCIPLE_NOT_FOUND	2691	0xa83	The Vserver principle not found
NSERR_KCD_REM_INUSE	2692	0xa84	KCD account is in use and cannot be removed

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_KCD_TOO_MANY_VS_PRINCIPLE	2693	0xa85	Too many host principles
NSERR_WI_REFRESH_NOT_SITEWEB	2694	0xa86	Show Refresh Attribute supported only for site type XenAppWeb
NSERR_WI_UIMODE_NOT_SITEWEB	2695	0xa87	User Interface Mode Attribute supported only for site type XenAppWeb
NSERR_WI_UILAYOUT_NOT_SITEWEB	2696	0xa88	User Interface Layout Attribute supported only for site type XenAppWeb
NSERR_WI_MESSAGESTRS_NOT_SITEWEB	2697	0xa89	App Welcome Message, Welcome Message, Footer Text, Login Sys Message, Pre Login Button, Pre Login Message, Pre Login Title Attributes supported only for site type XenAppWeb
NSERR_AAATM_AUTHN_PROFILE_CONF	2704	0xa90	Please turn ON authentication or authn401 setting in order to use authentication profile
NSERR_NEGACTION_UNAME_DOM	2705	0xa91	Domain must either be specified either

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
			explicitly or in the username
NSERR_NO_PRODUCTION_FARM	2706	0xa92	WI site will not be functional till a production farm is bound
NSERR_SAML_FORM_CONFLICT	2707	0xa93	Traffic cannot have both SAML SSO and Form SSO on same action
NSERR_MAXLOGIN_FAILLOGIN_CONFLICT	2708	0xa94	Please specify both max login attempts and fail login timeout
NSERR_KCD_ACCOUNT_EXIST	2709	0xa95	The KCD account does not exist
NSERR_KCD_ACCOUNT_NOTCONFIGURED	2710	0xa96	The KCD account is not configured
NSERR_NEGACTION_KEYTAB_CONFLICT	2711	0xa97	Action should have either keytab file or domain, username and password. Domain need not be specified if UPN is given for username
NSERR_KEYTAB_INVALID_ENC	2712	0xa98	Unsupported encryption type in keytab file
NSERR_HTTP_SSL_PROXY_CONFLICT	2713	0xa99	Cannot configure both HTTP and SSL proxy

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_INVALIDIP_PORT	2714	0xa9a	Invalid IP or Port
NSERR_ADVEPA_NOTSUPP	2715	0xa9b	VServer does not support advanced EPA scans
NSERR_ADVEPA_NOPROFILE	2716	0xa9c	EPA profile with this name does not exist
NSERR_ADVEPA_INUSE	2717	0xa9d	Bound EPA profile cannot be removed.
NSERR_ADVEPA_EXISTS	2718	0xa9e	EPA profile exists.
NSERR_ADVEPA_BOUND	2719	0xa9f	EPA profile already bound to vserver.
NSERR_ADVEPA_NOTBOUND	2720	0xaa0	EPA profile not bound to vserver.
NSERR_ADVEPA_ON	2721	0xaa1	Advanced EPA is ON, can not bind classic preauthentication policy.
NSERR_DEVICEPROFILE_ADDRM_FAIL	2722	0xaa2	There has been a design change in the support of OPSWAT specific EPA scans. EPA Profile Configuration is no longer needed. Please refer to support documents for complete details.

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_DEVICEPROFILE_INTERNAL_ERR	2723	0xaa3	An Internal Error occurred while operating on the Device Profile, please contact your Admin
NSERR_AAA_SESS_INVALID_INDEX	2724	0xaa4	Invalid attribute index. Attribute index should be between 1 and 16 both included
NSERR_AAATM_FORCETIMEOUT	2725	0xaa5	Force timeout setting of START or RESET must accompany a desired time in minutes
NSERR_KCDACCOUNT_KEYTAB	2726	0xaa6	Keytab file cannot be specified along with other parameters in kcdaccount
NSERR_KCDACCOUNT_REALM	2727	0xaa7	Realm must be specified by itself or extracted from delegated username/ keytab
NSERR_KCDACCOUNT_KEYTAB_INVALID	2238	0x8be	Invalid Keytab file
NSERR_WEBAUTH_FULLEXP	2728	0xaa8	Please specify full request expression
NSERR_WI_INVALID_SETTING_FOR_AUTHPOINT	2729	0xaa9	Setting is Invalid for given Authpoint

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_WI_SETTING_VALIDONLYFOR_XENAPPWEB	2730	0xaaa	Setting is Invalid for SiteType other than XenAppWeb
NSERR_WI_PARAMETER_UPGARDE_ERROR	2731	0xaab	Migration of WebInterface.conf parameter to CLI didn't happen successfully
NSERR_SAMLIDP_ENC_CERT	2732	0xaac	Encryption option requires ServiceProvider (SP) certificate.
NSERR_WF_NOT_INST	2733	0xaad	Web Front is not installed
NSERR_WF_INSTFAILED	2734	0xaae	Installation failed. Please check the log file /var/log/wfcmd.log
NSERR_AAA_TOOMANY_EXP	2735	0xaaf	Number of expressions found exceeds allowed limit
NSERR_SAML_REDIR_CONFLICT	2736	0xab0	Signature and Digest algorithms are incompatible for Redirect Binding
NSERR_SET_MAXAAAUSER_NOT_ALLOWED	2737	0xab1	Set maxaaaUser not allowed per partition
NSERR_AAATM_INCOMP_NO_PROFILE	2744	0xab8	Profile does not exist or does not have Host configured

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_RENAME_AUTHN_LABEL_NOT_PERMITTED	2745	0xab9	Rename of authentication policyLabel not permitted if it referred as nextFactor
NSERR_ERR_AAA_LICENSE_LOW	2747	0xabb	MaxAAAUsers value less than allowed by license, ignored.
NSERR_ERR_ENABLE_DTLS	2750	0xabe	Cannot start DTLS or PCOIP listener due to existing (ip, port, transport) conflicts.
NSERR_OPENID_ENC_METADATA	2751	0xabf	Token encryption requires Relying Party metadata url.
NSERR_OPENID_MAX_ATTRIBUTES	2814	0xafe	Expression exceeds maximum permissble attributes.
NSERR_AAA_MAX_LIMIT	2815	0xaff	It's taking longer than expected. Not processing further entries.

SST ERRORS

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_SST_SUBSCR_ALLOC_FAILED	3504	0xdb0	Cannot allocate memory for subscriber in extended memory space

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_SST_SUBSCR_LOOKUP_FAILED	3505	0xdb1	Cannot find subscriber
NSERR_SST_SUBSCR_REQUEST_ERROR	3506	0xdb2	Invalid request for subscriber
NSERR_GX_SERVICE_CONFIG_XOR	3507	0xdb3	service and vserver cannot be set at the same time.
NSERR_GX_NOT_DIAMETER_VS	3508	0xdb4	Not a DIAMETER or SSL_DIAMETER vserver.
NSERR_GX_NOT_DIAMETER_SERVICE	3509	0xdb5	Not a DIAMETER or SSL_DIAMETER service.
NSERR_SST_SUBSCRIBER_ENTRY_EXCEEDED	3510	0xdb6	Size of subscriber entry exceeds total allowed size.
NSERR_GX_PCRF_NOT_CONFIGURED_VSERVER_SERVICE	3511	0xdb7	PCRF not configured. To configure PCRF, please use set gxInteface -vserver/service .
NSERR_SST_STATIC_SUBSCRIBER_SESSION_DELETION	3512	0xdb8	Static subscriber profiles cannot be deleted using this command, please use 'rm subscriber profile'

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_SST_SUBSCRIBER_SESSION_EXIST	3513	0xdb9	subscriber profile cannot be added as corresponding subscriber session already exists
NSERR_SST_NOT_RADIUS_SERVICE	3514	0xdba	Not RADIUS Listener service
NSERR_MAX_SERVICE_FUNCTIONS	3515	0xdbb	Number for service functions exceeding the limit
NSERR_NOSUCH_SVCFUNC	3516	0xdbc	Service Function is not present with specified name
NSERR_NOSUCH_SVCPATH	3517	0xdbd	Service Path is not present with specified name
NSERR_INVALID_SVCINDEX	3518	0xdbe	The value of service index is invalid
NSERR_SVCPATH_SVCINX_EXISTS	3519	0xdbf	A service function is already bound with given service index

SST ERRORS2

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_SST_IPANDVLAN_GXONLY	3799	0xed7	IPANDVLAN keytype can only be set in GxOnly interface type mode.
NSERR_VLAN_NOT_ALLOWED_DEFAU	3800	0xed8	VLAN ID is not allowed for the

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
LT_SUBSCRIBER_PROFILE			default subscriber profile.

SVPN ERRORS

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSCFG_INFO	2049	0x801	Sending the /cfg information
NSCS_INFO	2050	0x802	Backend server info exists
NSCSPROBE_INFO	2051	0x803	Probe to backend server pending
NSAPPPROBE_INFO	2052	0x804	Client side connection being closed
NSCFG_MP_INFO	2112	0x840	Sending the /mp_cfg Information
NSERR_NOINTRANETIP	2113	0x841	No Intranet IP available
NSERR_ALREADYLOGEDIN	2114	0x842	The user is already logged-in
NSERR_URLINUSE	2115	0x843	Bound URL/ bookmark cannot be removed.
NSERR_VPNAPPINUSE	2116	0x844	Bound VPN application cannot be removed.

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_NOTSUPP_TRANS_INTERCPT	2117	0x845	Transparent interception is not yet supported.
NSERR_CLNT_CERT_RENEG	2118	0x846	Client SSL certificate renegotiation failed
NSERR_DEFAULTCMDPLCY	2119	0x847	Default command policy cannot be removed
NSERR_CLNT_CERT_REQD	2120	0x848	Client SSL certificate is required
NSERR_INVAL_CERTFIELD	2121	0x849	Invalid certificate field
NSERR_VPNAPP_PROXY_IPRANGE	2064	0x810	Proxy interception does not support IP ranges
NSERR_VPNAPP_PROXY_NETMASK	2065	0x811	Proxy interception does not support netmasks
NSERR_VPNAPP_PROXY_DSTPORT_RANGE	2066	0x812	Proxy interception does not support destination port ranges
NSERR_VPNAPP_PROXY_PROTOCOL	2067	0x813	Proxy interception supports only TCP
NSERR_VPNAPP_PROXY_HOSTNAME	2068	0x814	Proxy interception does not support hostname interception

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_VPNAPP_TRANS_SRCIP	2069	0x815	Transparent interception does not support source IP
NSERR_VPNAPP_TRANS_SRCPORT	2070	0x816	Transparent interception does not support source port
NSERR_VPNAPP_NO_INTERCEPTION_TYPE	2071	0x817	Intranet application requires an interception type
NSERR_VPNAPP_CLIAPP_PORT	2072	0x818	Both client application name and destination port cannot be specified
NSERR_VPNAPP_CLIAPP_PROTO	2073	0x819	Protocol can not be specified when client application name is present
NSERR_VPNAPP_PROXY_CLIAPP	2074	0x81a	Proxy interception does not support client application based interception
NSERR_VPNAPP_MISSING_PROTO	2075	0x81b	Protocol must be specified
NSERR_VPNAPP_MISSING_ARG	2076	0x81c	One of destIP, IPRange or hostname has to be specified
NSERR_VPNAPP_TOO_MANY_ARG	2077	0x81d	At most one of destIP, IPRange or hostname may be specified

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_FS_AUTHFAIL	2078	0x81e	
NSERR_NSIPV6NOTPRESENT	2079	0x81f	No IPV6 NetScaler IP has been configured
NSERR_REMOVE_SESSION	2096	0x830	No IPV6 NetScaler IP has been configured
NSERR_STAWI_EXIST	3250	0xcb2	A STA or WI DBS configuration exists. Unset it first
NSERR_INVALID_SSO_ACTION	2099	0x833	Invalid sso action
NSERR_INVALID_TMTRAFFIC_ACTION	2100	0x834	Invalid tm traffic action
NSERR_INVALFSSO	2101	0x835	SSO should be turned on for setting formsso action
NSERR_INVALIDURL	2102	0x836	Action url should be root relative url
NSERR_INVALID_FLOWTYPE_FORAPPFLOW	2126	0x84E	Flowtype needs to be REQUEST or ICA_REQUEST or OTHERTCP_REQUEST for appflow policy when bound to VPN vservers
NSERR_TOO_MANY_SERVERS	2127	0x84F	Too many servers bound

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_BLOCKING_ATTR_WARNING_FOR_VPN_APPFLOW	2961	0xb91	Policy will not apply to VPN traffic if it has blocking attributes
NSERR_SAMLIDP_ACTION	2975	0xb9f	Invalid SAML IDP Action
NSERR_SAML_ACTION_AUTHNCTX	2976	0xba0	None option is mutually exclusive with other Authentication Class References
NSERR_ABSOLUTE_URL	2977	0xba1	URL has to be an absolute URL
NSERR_INVALID_AG_BIND	2978	0xba2	SSLVPN vserver can be bound to only SSL type CS vserver
NSERR_NO_VSERVER	2979	0xba3	Please specify the associated vserver name
NSERR_SSSO_NOT_LICENSED	2980	0xba4	This feature needs enterprise or platinum license.
NSERR_MULT_AGBIND	2981	0xba5	Only one VPN vserver can be bound to a CS vserver.
NSERR_VPN_VSERV_PROTOCOL_NOT_ALLOWED	2982	0xba6	VPN/Authentication Vserver of service type 'HTTP' is not allowed.

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_SET_NOT_ALLOWED_ON_ICA ONLY_BIT	2983	0xba7	Changing 'ICAonly' parameter is not allowed in Cluster Deployment.
NSERR_IIP_INVALI D_RANGE	2984	0xba8	The given intranet IP binding does not exist
NSERR_SSLVPN_LI CENSE	2985	0xba9	Feature not licensed [SSLVPN]
NSERR_SAMLIDP_ REDIR_INVALID_SI GN	2990	0xbae	signAssertion option can only be set to ASSERTION in Redirect binding
NSERR_VPN_AUTH _BIND	2991	0xbaf	Authentication vserver can not be bound to a CS vserver if VPN vserver is already bound to it.
NSERR_AUTH_VPN _BIND	2992	0xbb0	VPN vserver can not be bound to a CS vserver if Authentication vserver is already bound to it.
NSERR_SVPN_INV ALID_URL	2993	0xbb1	URL must be an absolute url with a trailing slash
NSERR_MULT_AUT HBIND	2994	0xbb2	Only one Authentication vserver can be bound to a CS vserver.

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_SVPN_INVALID_ICONURL	2995	0xbb3	Only the following image types i.e. .png, .jpeg, .jpg and .giff are allowed as bookmark icons.
NSERR_XM_PKG_CONTENT	2996	0xbb4	XenMobile package content error. Please find more information in /var/log/nsxm.log
NSERR_XM_MISSING_TOKEN_VALUE	2997	0xbb5	XenMobile script tokens replacement failure. Please find more information in /var/log/nsxm.log
NSERR_SAML_ARTIFACT_NO_URL	2998	0xbb6	Artifact resolution url is required when binding is specified as ARTIFACT
NSERR_OAUTHIDP_ACTION	2999	0xbb7	Invalid OAuth IDP Action
NSERR_NOLICENCE_PUSH	3000	0xbb8	Platinum license is required for this operation
NSERR_INVALSAMLSSO	3001	0xbb9	SSO should be turned on for setting samlsso action
NSERR_INVALSAMLIDPATTR1	2512	0x9d0	Incorrect expression at attribute 1
NSERR_INVALSAMLIDPATTR2	2513	0x9d1	Incorrect expression at attribute 2

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_INVALSAMLIDPATTR3	2514	0x9d2	Incorrect expression at attribute 3
NSERR_INVALSAMLIDPATTR4	2515	0x9d3	Incorrect expression at attribute 4
NSERR_INVALSAMLIDPATTR5	2516	0x9d4	Incorrect expression at attribute 5
NSERR_INVALSAMLIDPATTR6	2517	0x9d5	Incorrect expression at attribute 6
NSERR_INVALSAMLIDPATTR7	2518	0x9d6	Incorrect expression at attribute 7
NSERR_INVALSAMLIDPATTR8	2519	0x9d7	Incorrect expression at attribute 8
NSERR_INVALSAMLIDPATTR9	2520	0x9d8	Incorrect expression at attribute 9
NSERR_INVALSAMLIDPATTR10	2521	0x9d9	Incorrect expression at attribute 10
NSERR_INVALSAMLIDPATTR11	3002	0xbba	Incorrect expression at attribute 11
NSERR_INVALSAMLIDPATTR12	2523	0x9db	Incorrect expression at attribute 12
NSERR_INVALSAMLIDPATTR13	2524	0x9dc	Incorrect expression at attribute 13
NSERR_INVALSAMLIDPATTR14	2525	0x9dd	Incorrect expression at attribute 14
NSERR_INVALSAMLIDPATTR15	2526	0x9de	Incorrect expression at attribute 15
NSERR_INVALSAMLIDPATTR16	2527	0x9df	Incorrect expression at attribute 16

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_PUSH_SERVICE_AZURE_ARGS	2550	0x9f6	Azure type service requires Namespace, Hub, Servicekey and Servicekey name but not Trust service
NSERR_PUSH_SERVICE_NS_ARGS	2551	0x9f7	Citrix type service requires Client id and secret
NSERR_INVALID_DFA_BINDPOINT	2552	0x9f8	DFA policies cannot be bound to user defined policylabels/ factors
NSERR_SMARTACCESS_ACTION	2313	0x909	Invalid Smartaccess profile
NSERR_ROLLOVER_DNSKEY_NOT_ACTIVE	2330	0x91A	Key should be in activated state for rollover. Please use sign dns zone operation to activate the key
NSERR_WRONG_ROLLOVER_METHOD	2331	0x91B	Rollover method is wrong for key type
NSERR_ROLLOVER_TOO_SHORT	2332	0x91C	Notification (rollover) period is too short
NSERR_DNSKEY_NOROLLOVER	2333	0x91D	Please enable autosync in GSLB parameter for rollover to happen

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_DNSKEY_REVOKE_NOTALLOWED	2334	0x91E	Revoke operation not allowed, key not active
NSERR_DNSKEY_CONFIG_NOTSAVED	2304	0x900	Please enable autosaveKeyOps in DNS parameter to avoid config loss
NSERR_ROLLOVER_BACKUP_KEY_EXISTS	2346	0x92A	Successor key already exists
NSERR_ROLLOVER_REVOKED_DNSKEY	2347	0x92B	Rollover not allowed for revoked keys
NSERR_DNSKEY_REVOKE_FAILED	2348	0x92C	Revoke operation failed because of memory allocation failure

TD ERRORS

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_TD_EXISTS	944	0x3b0	The specified traffic domain is already configured.
NSERR_TD_VLAN	945	0x3b1	The specified VLAN/VXLAN/bridge group is already bound to another traffic domain. These entities can belong to only one traffic domain.

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_TD_NOTEXIST	946	0x3b2	The specified traffic domain is not configured.
NSERR_TD_MISMATCH_WITH_L3VLAN	947	0x3b3	L3 VLANs can not be bound to a traffic domain.
NSERR_TD_MISMATCH	948	0x3b4	The binding entities have incompatible traffic domain identifiers.
NSERR_TD_NOSUPP	949	0x3b5	This feature is not supported in a non-default traffic domain.
NSERR_TD_CONFIG_NOT_ALLOWED	950	0x3b6	This configuration option is not supported in a non-default traffic domain.
NSERR_TD_IP_NOTEXIST	951	0x3b7	The IP address is not configured for the specified traffic domain.
NSERR_TD_VLAN_NOTEXIST	952	0x3b8	The specified VLAN is not configured.
NSERR_TD_DEFVLAN	953	0x3b9	Default VLAN cannot be bound/unbound to/from traffic domain.
NSERR_TD_BDG_NOTEXIST	954	0x3ba	The specified bridge group is not configured.

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_TD_VLAN_BDG_EXIST	955	0x3bb	The specified VLAN is bound to a bridge group.
NSERR_TD_SERVER_MISMATCH	956	0x3bc	The specified virtual server already bound to a service in a different traffic domain.
NSERR_DIFF_TD_NALLOWED_LLB	957	0x3bd	Not allowed for LLB: Services bound to the specified virtual server must be in same traffic domain.
NSERR_DUPIP	958	0x3be	IP address duplication with VMAC address detected. Please try a different IP address.
NSERR_VMAC_VLAN	959	0x3bf	Traffic domain can be either VLAN based or VMAC based.
NSERR_TD_SYNCVLAN	960	0x3c0	SYNC VLAN cannot be bound/unbound to/from traffic domain.
NSERR_TD_NOT_VLAN	961	0x3c1	The specified VLAN/VXLAN/bridge group is not bound to given traffic domain.
NSERR_SYNCNSVLAN_TD	975	0x3cf	VLAN bound to traffic domain cannot

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
			be configured as SYNC/NS VLAN.
NSERR_TD_CONFIG_DEPR	934	0x3a6	Traffic domains related configuration commands are deprecated and will be removed in a future release. Citrix recommends that you use admin partitions instead of using traffic domains.

URLFILT ERRORS

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_URLFILT_CANNOT_PARSE_XML	3772	0xebc	Cannot parse XML categories file.
NSERR_URLFILT_CANNOT_FIND_GROUP	3773	0xebd	Cannot find the specified category group.
NSERR_URLFILT_XML_FILE_TOO_BIG	3774	0xebe	XML categories file is too big.
NSERR_URLFILT_DEPRECATED_IC_CACHE_NOT_ENABLED	3869	0xf1d	URLFiltering feature is no longer supported.
NSERR_URLFILT_DEPRECATED	1720	0x6b8	URLFiltering feature is no longer supported.

URLSET ERRORS

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_URLSET_CANNOT_INIT_PATTERN	3768	0xeb8	Cannot initialize urlset pattern.
NSERR_URLSET_CANNOT_FIND_URL	3769	0xeb9	Cannot find url in urlset.

URLTRANS ERRORS

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_URLTRANS_MAX_ENTITIES	2960	0xb90	Number of URL Transformation entities exceeds limit
NSERR_URLTRANS_INVAL_PROFILE	2962	0xb92	Invalid URL Transformation profile
NSERR_URLTRANS_ACTION_INUSE	2963	0xb93	Action name is already in use
NSERR_URLTRANS_PRIORITY_EXISTS	2964	0xb94	An object with this priority already exists
NSERR_URLTRANS_REQ_PCRE_ERR	2965	0xb95	Invalid PCRE expression under 'reqUrlFrom'
NSERR_URLTRANS_RESP_PCRE_ERR	2966	0xb96	Invalid PCRE expression under 'resUrlFrom'
NSERR_URLTRANS_REQ_INTO_ERR	2967	0xb97	Invalid expression under 'reqUrlInto'

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_URLTRANS_RESP_INTO_ERR	2968	0xb98	Invalid expression under 'resUrlInto'
NSERR_URLTRANS_COOKIE_INTO_ERR	2969	0xb99	Invalid expression under 'cookieDomainInto'
NSERR_URLTRANS_COOKIE_PCRE_ERR	2970	0xb9a	Invalid PCRE expression under 'cookieDomainFrom'
NSERR_URLTRANS_TOO_MANY_BACKREFS	2971	0xb9b	More than 5 back references in PCRE expression
NSERR_URLTRANS_MISSING_FROM	2972	0xb9c	Each 'Into' expression must have a corresponding 'From' pattern
NSERR_URLTRANS_NOT_SUPPORTED_VS	2973	0xb9d	Specified policy can be bound only to HTTP/SSL/PROXY/HTTP_QUIC type vserver
NSERR_URLTRANS_BAD_COMMENT	2974	0xb9e	Invalid comment

VIDEOOPT ERRORS

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_VIDEOOPT_INV_RANDOMSAMPLING	3804	0xedc	Invalid RandomSampling parameter. Should be >=0.0 and <=100.0

VLAN ERRORS

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_INTERFACEBOUND	2080	0x820	Interface is already bound to this VLAN
NSERR_IFACE_NO_UNBIND	2081	0x821	Untagged interface cannot be removed from default VLAN. To remove, bind to other VLAN.
NSERR_IFACE_MAX_VLANS	2082	0x822	Maximum number of tagged VLANs bound to the interface exceeded or the binding of this VLAN is not allowed on the interface.
NSERR_VLAN_RTEXIST	2083	0x823	An existing route relies on the presence of this vlan
NSERR_VLAN_LLEXIST	2084	0x824	An existing link-local ip relies on the presence of this vlan
NSERR_BOUNDTONSVLAN	2085	0x825	Interface/Channel bound to NSVLAN
NSERR_VLAN_TD_CONFIGURED	2408	0x968	TD is configured on this bridgegroup/ vlan. Cannot delete this
NSERR_VLAN_BOUNDTO_NETBRIDGE	1216	0x4c0	Vlan bound to Netbridge cannot be removed

VMAC ERRORS

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_INTERFACE_BOUND	3329	0xd01	Interface already bound
NSERR_VRID_INTERFACE_NOT_BOUND	3330	0xd02	Interface not bound
NSERR_NO_SUCH_INTERFACE	3331	0xd03	No such interface
NSERR_DYNAMIC_ENTRY	3346	0xd12	Dynamic Entry exists.
NSERR_PRIO_INTFVRID	3347	0xd13	Invalid Priority for interface bound VRID
NSERR_INTFVRID	3348	0xd14	Binding interface is not allowed for Dynamic or IP bound VRID
NSERR_NOTSTATIC_VRID	3349	0xd15	Not a Configured VRID
NSERR_IPVRID	3350	0xd16	IP binding is not allowed for Interface VRID
NSERR_IPVRID_BOUND	3351	0xd17	VRID already bound to this IP
NSERR_NOVRID	3354	0xd1a	VRID doesn't exist
NSERR_INTF_TRACKINTF_BOUND	3362	0xd22	Interfaces can either be tracked or bound to a vrID.

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_VRRP_SHAREDVLAN_NOT_SUPPORTED	3408	0xd50	VRRP functionality is not supported on shared VLANs.
NSERR_INTF_VRID_BIND_NOTALLOWED	3868	0xf1c	Binding of interface to this VRID is not allowed. Please check if the VRID is allowed for the interface from SVM.

VXLAN ERRORS

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_VXLAN_INCOMP	2608	0xa30	Vlan extension and IP address - both cannot be configured on vxlan
NSERR_VXLAN_TUN_BOUND	2609	0xa31	Tunnel is already bound to this vxlan
NSERR_INV_MCAST	2610	0xa32	Another multicast group already configured for this vxlan
NSERR_TUN_NOT_BOUND	2611	0xa33	Tunnel not bound to this vxlan
NSERR_IP_NOT_BOUND	2612	0xa34	IP/IPv6 address not bound to this vxlan
NSERR_INV_TUN	2613	0xa35	Tunnel should be of VXLAN type
NSERR_NO_VXLAN	2614	0xa36	Vxlan is not configured

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_VLAN_EXT	2615	0xa37	Vlan already extended by a different vxlan
NSERR_VXLAN_TD	2616	0xa38	Vxlan is bound to a traffic domain
NSERR_VXLAN_ROTUING	2617	0xa39	Vlan extension and routing - both cannot be configured on vxlan
NSERR_VXLANMAP_INUSE	2743	0xab7	This vlan-to-vxlan map table is in use by a netbridge/pbr-tunnel
NSERR_VXLAN_TBL_BOUND	2738	0xab2	Vxlan is in use by a vlan-to-vxlan map table
NSERR_TUN_MAP_TBL	2739	0xab3	The tunnel currently applies vlan-to-vxlan mappings
NSERR_VXLAN_INUSE	2740	0xab4	Vxlans that have vlan extensions or IP addresses or routing cannot be used in mapping table
NSERR_NETBDG_VXLAN_VLAN	2741	0xab5	Vlan-to-vxlan map table and vlan - both cannot be configured on a netbridge
NSERR_NO_VXLANMAP	2742	0xab6	Vlan-to-vxlan map table is not configured

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_VXLANMAP_TUN_NOSUP	2746	0xaba	Incompatible tunnel type for vlan-to-vxlan map table

WARNING

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE

WARNING ERRORS

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_AUTHORIZE		NS_WARNING| 0x001	
NSERR_AUTHFAIL		NS_WARNING| 0x002	
NSWAR_SSL_BINDOR		NS_WARNING| NSERR_SSL_BINDOR	Current certificate replaces the previous binding
NSWAR_SSL_BRKLINK		NS_WARNING| NSERR_SSL_BRKLINK	All incompatible CA links/Cert Bindings were broken during the update operation
NSWAR_SSL_CERT_NOT_YET_VALID		NS_WARNING| NSERR_SSL_CERT_NOT_YET_VALID	The specified certificate is not yet valid
NSWAR_SSL_CERT_EXPIRED		NS_WARNING| NSERR_SSL_CERT_EXPIRED	The certificate has expired

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSWAR_SSL_EXPIRED_BRKLINK		NS_WARNING| NSERR_SSL_EXPIRED_BRKLINK	All incompatible CA links were broken during the update operation. (Note: the certificate has expired)
NSWAR_SSL_NYVALID_BRKLINK		NS_WARNING| NSERR_SSL_NYVALID_BRKLINK	All incompatible CA links were broken during the update operation. (Note: the certificate is not yet valid)

XS ERRORS

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_CIPROF_INTERFACE_NOT_ALLOWED	2436	0x984	IngressInterface and Ingressvlan are not allowed for this contentinspection profile type
NSERR_XS_INTERNAL_RESOURCE_CREATION	3794	0xed2	Resource creation failed, internal error.
NSERR_XS_INVALID_SERVERNAME	3795	0xed3	Unsupported service type. Supported types are TCP and SSL_TCP for ICAP, TCP for INLINEINSPECTION and ANY for MIRROR.

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_CI_ACT_IP_PORT_NOT_ALLOWED	3820	0xeec	IP and Port can't set be for this contentinspection action type
NSERR_CI_ACT_SNAME_SIP_CONFLICT	3796	0xed4	Server name and ip can't both be set for this content inspection entity.
NSERR_XS_INVALID_ICAPPROFILE_NAME	3797	0xed5	Invalid ICAP profile name.
NSERR_CI_PROFILE_EXISTS	3798	0xed6	ContentInspection profile exists with the given name.
NSERR_CIPROF_INUSE	3801	0xed9	Can't change MODE as the ContentInspection profile is in use.
NSERR_XS_INVALID_CIPROFILE_NAME	3766	0xeb6	Invalid contentInspection profile name.
NSERR_CI_UNSUPPORTED_PROFILE_TYPE	3767	0xeb7	Invalid Content Inspection type specified.
NSERR_CI_NO_PROFILE	3817	0xee9	Content Inspection profile does not exist.
NSERR_CI_INVALID_CIC	3821	0xeed	Content Inspection callout does not exist or type didn't match.

ERROR CODE	ERROR CODE(DECIMAL)	ERROR CODE(HEX)	ERROR MESSAGE
NSERR_CI_ACT_MISSING_PROFILE	3823	0xeef	ContentInspectionProfile is not set on service(s)
NSERR_CIPROF_TUNNEL_NOT_ALLOWED	2437	0x985	Tunnel is not allowed for this contentinspection profile type

index

- API Reference
- service
- cspolicy
- csvserver
- csvserver_cspolicy_binding
- lbvserver
- lbvserver_service_binding
- sslcertkey
- sslvserver_binding

API Reference

This documentation provides details of all operations that can be performed on the NetScaler appliance by using the REST API.

- Configuration
- Statistics
- Error Messages

service

Configuration for service resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the service. Must begin with an ASCII

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the service has been created. Minimum length = 1
ip	<String>	Read-write	IP to assign to the service. Minimum length = 1
servername	<String>	Read-write	Name of the server that hosts the service. Minimum length = 1
servicetype	<String>	Read-write	Protocol in which data is exchanged with the service. Possible values = HTTP, FTP, TCP, UDP, SSL, SSL_BRIDGE, SSL_TCP, DTLS, NNTP, RPCSVR, DNS, ADNS, SNMP, RTSP, DHCPRA, ANY, SIP_UDP, SIP_TCP, SIP_SSL, DNS_TCP,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			ADNS_TCP, MYSQL, MSSQL, ORACLE, MONGO, MONGO_TLS, RADIUS, RADIUSListener, RDP, DIAMETER, SSL_DIAMETER, TFTP, SMPP, PPTP, GRE, SYSLOGTCP, SYSLOGUDP, FIX, SSL_FIX, USER_TCP, USER_SSL_TCP, QUIC, IPFIX, LOGSTREAM, LOGSTREAM_SSL, MQTT, MQTT_TLS, QUIC_BRIDGE, DOT, ADNS_DOT, HTTP_QUIC, ADNS_DOH, KAFKA_BROKER
port	<Integer>	Read-write	Port number of the service. Range 1 - 65535 * in CLI is represented as 65535 in NITRO API
cleartextport	<Integer>	Read-write	Port to which clear text data must be sent after the appliance decrypts incoming SSL traffic.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Applicable to transparent SSL services. Minimum value = 1
cachetype	<String>	Read-write	Cache type supported by the cache server. Possible values = TRANSPARENT, REVERSE, FORWARD
maxclient	<Integer>	Read-write	Maximum number of simultaneous open connections to the service. Minimum value = 0 Maximum value = 4294967294
healthmonitor	<String>	Read-write	Monitor the health of this service. Available settings function as follows: YES - Send probes to check the health of the service. NO - Do not send probes to check the health of the service. With the NO option, the appliance shows the service as UP at all times.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: YES Possible values = YES, NO
maxreq	<Integer>	Read-write	Maximum number of requests that can be sent on a persistent connection to the service. Note: Connection requests beyond this value are rejected. Minimum value = 0 Maximum value = 65535
cacheable	<String>	Read-write	Use the transparent cache redirection virtual server to forward requests to the cache server. Note: Do not specify this parameter if you set the Cache Type parameter. Default value: NO Possible values = YES, NO
cip	<String>	Read-write	Before forwarding a request to the service, insert an HTTP header with the client's IPv4 or IPv6 address as its

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			value. Used if the server needs the client's IP address for security, accounting, or other purposes, and setting the Use Source IP parameter is not a viable option. Possible values = ENABLED, DISABLED
cipheader	<String>	Read-write	Name for the HTTP header whose value must be set to the IP address of the client. Used with the Client IP parameter. If you set the Client IP parameter, and you do not specify a name for the header, the appliance uses the header name specified for the global Client IP Header parameter (the cipHeader parameter in the set ns param CLI command or the Client IP Header parameter in the Configure HTTP Parameters dialog box at System > Settings > Change HTTP parameters). If the global Client IP Header parameter is

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			not specified, the appliance inserts a header with the name "client-ip.". Minimum length = 1
usip	<String>	Read-write	Use the client's IP address as the source IP address when initiating a connection to the server. When creating a service, if you do not set this parameter, the service inherits the global Use Source IP setting (available in the enable ns mode and disable ns mode CLI commands, or in the System > Settings > Configure modes > Configure Modes dialog box). However, you can override this setting after you create the service. Possible values = YES, NO
pathmonitor	<String>	Read-write	Path monitoring for clustering. Possible values = YES, NO
pathmonitorindv	<String>	Read-write	Individual Path monitoring decisions.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = YES, NO
useproxyport	<String>	Read-write	Use the proxy port as the source port when initiating connections with the server. With the NO setting, the client-side connection port is used as the source port for the server-side connection. Note: This parameter is available only when the Use Source IP (USIP) parameter is set to YES. Possible values = YES, NO
sp	<String>	Read-write	Enable surge protection for the service. Possible values = ON, OFF
rtspsessionidremap	<String>	Read-write	Enable RTSP session ID mapping for the service. Default value: OFF Possible values = ON, OFF
clttimeout	<Integer>	Read-write	Time, in seconds, after which to

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			terminate an idle client connection. Minimum value = 0 Maximum value = 31536000
svrtimeout	<Integer>	Read-write	Time, in seconds, after which to terminate an idle server connection. Minimum value = 0 Maximum value = 31536000
customserverid	<String>	Read-write	Unique identifier for the service. Used when the persistency type for the virtual server is set to Custom Server ID. Default value: "None"
serverid	<Integer>	Read-write	The identifier for the service. This is used when the persistency type is set to Custom Server ID.
cka	<String>	Read-write	Enable client keep-alive for the service. Possible values = YES, NO
tcpb	<String>	Read-write	Enable TCP buffering for the service.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = YES, NO
cmp	<String>	Read-write	Enable compression for the service. Possible values = YES, NO
maxbandwidth	<Integer>	Read-write	Maximum bandwidth, in Kbps, allocated to the service. Minimum value = 0 Maximum value = 4294967287
accessdown	<String>	Read-write	Use Layer 2 mode to bridge the packets sent to this service if it is marked as DOWN. If the service is DOWN, and this parameter is disabled, the packets are dropped. Default value: NO Possible values = YES, NO
monthreshold	<Integer>	Read-write	Minimum sum of weights of the monitors that are bound to this service. Used to determine whether to mark a service as UP or DOWN. Minimum value = 0

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum value = 65535
state	<String>	Read-write	Initial state of the service. Default value: ENABLED Possible values = ENABLED, DISABLED
downstateflush	<String>	Read-write	Flush all active transactions associated with a service whose state transitions from UP to DOWN. Do not enable this option for applications that must complete their transactions. Default value: ENABLED Possible values = ENABLED, DISABLED
tcpprofilename	<String>	Read-write	Name of the TCP profile that contains TCP configuration settings for the service. Minimum length = 1 Maximum length = 127

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
httpprofilename	<String>	Read-write	Name of the HTTP profile that contains HTTP configuration settings for the service. Minimum length = 1 Maximum length = 127
contentinspectionprofilename	<String>	Read-write	Name of the ContentInspection profile that contains IPS/IDS communication related setting for the service. Minimum length = 1 Maximum length = 127
aigwprofilename	<String>	Read-write	Name of the AIGW Profile that contains AIGW Endpoint setting for the service. Minimum length = 1 Maximum length = 255
quicprofilename	<String>	Read-write	Name of QUIC profile which will be attached to the service. Minimum length = 1 Maximum length = 255

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
hashid	<Integer>	Read-write	A numerical identifier that can be used by hash based load balancing methods. Must be unique for each service. Minimum value = 1
comment	<String>	Read-write	Any information about the service.
appflowlog	<String>	Read-write	Enable logging of AppFlow information. Default value: ENABLED Possible values = ENABLED, DISABLED
netprofile	<String>	Read-write	Network profile to use for the service. Minimum length = 1 Maximum length = 127
td	<Integer>	Read-write	Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0. Minimum value = 0

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum value = 4094
processlocal	<String>	Read-write	By turning on this option packets destined to a service in a cluster will not under go any steering. Turn this option for single packet request response mode or when the upstream device is performing a proper RSS for connection based distribution. Default value: DISABLED Possible values = ENABLED, DISABLED
dnsprofilename	<String>	Read-write	Name of the DNS profile to be associated with the service. DNS profile properties will applied to the transactions processed by a service. This parameter is valid only for ADNS, ADNS-TCP and ADNS-DOT services. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum length = 127
monconnectionclose	<String>	Read-write	Close monitoring connections by sending the service a connection termination message with the specified bit set. Default value: NONE Possible values = RESET, FIN
mcpprofilename	<String>	Read-write	Name of MCP profile which will be attached to the service.
ipaddress	<String>	Read-write	The new IP address of the service.
weight	<Integer>	Read-write	Weight to assign to the monitor-service binding. When a monitor is UP, the weight assigned to its binding with the service determines how much the monitor contributes toward keeping the health of the service above the value configured for the Monitor Threshold parameter. Minimum value = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum value = 100
monitor_name_svc	<String>	Read-write	Name of the monitor bound to the specified service. Minimum length = 1
delay	<Integer>	Read-write	Time, in seconds, allocated to the NetScaler for a graceful shutdown of the service. During this period, new requests are sent to the service only for clients who already have persistent sessions on the appliance. Requests from new clients are load balanced among other available services. After the delay time expires, no requests are sent to the service, and the service is marked as unavailable (OUT OF SERVICE).
graceful	<String>	Read-write	Shut down gracefully, not accepting any new connections, and disabling the service when all of its connections are closed.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: NO Possible values = YES, NO
all	<Boolean>	Read-write	Display both user-configured and dynamically learned services.
Internal	<Boolean>	Read-write	Display only dynamically learned services.
newname	<String>	Read-write	New name for the service. Must begin with an ASCII alphabetic or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Minimum length = 1
numofconnections	<Integer>	Read-only	This will tell the number of client side connections are still open.
policyname	<String>	Read-only	The name of the policyname for which this service is bound.
serviceconftype	<Boolean>	Read-only	The configuration type of the service.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
serviceconftype2	<String>	Read-only	The configuration type of the service (Internal/Dynamic/ Configured). Possible values = Configured, Dynamic, Internal
value	<String>	Read-only	SSL status. Possible values = Certkey/ Certkeybundle/Vault not bound/Cert-store not usable, SSL feature disabled
gslb	<String>	Read-only	The GSLB option for the corresponding virtual server. Possible values = REMOTE, LOCAL
dup_state	<String>	Read-only	Added this field for getting state value from table. Possible values = ENABLED, DISABLED
publicip	<String>	Read-only	public ip.
publicport	<Integer>	Read-only	public port. Minimum value = 1 Range 1 - 65535 * in CLI is represented as

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			65535 in NITRO API
svrstate	<String>	Read-only	The state of the service. Possible values = UP, DOWN, UNKNOWN, BUSY, OUT OF SERVICE, GOING OUT OF SERVICE, DOWN WHEN GOING OUT OF SERVICE, NS_EMPTY_STR, Unknown, DISABLED
monitor_state	<String>	Read-only	The running state of the monitor on this service. Possible values = UP, DOWN, UNKNOWN, BUSY, OUT OF SERVICE, GOING OUT OF SERVICE, DOWN WHEN GOING OUT OF SERVICE, NS_EMPTY_STR, Unknown, DISABLED
monstatcode	<Integer>	Read-only	The code indicating the monitor response.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
lastresponse	<String>	Read-only	The string form of monstatcode.
responsetime	<Integer>	Read-only	Response time of this monitor.
monstatparam1	<Integer>	Read-only	First parameter for use with message code.
monstatparam2	<Integer>	Read-only	Second parameter for use with message code.
monstatparam3	<Integer>	Read-only	Third parameter for use with message code.
statechangetimesec	<String>	Read-only	Time when last state change happened. Seconds part.
statechangetimemsec	<Integer>	Read-only	Time at which last state change happened. Milliseconds part.
tickssincelaststatechange	<Integer>	Read-only	Time in 10 millisecond ticks since the last state change.
stateupdatereason	<Integer>	Read-only	Checks state update reason on the secondary node.
clmonowner	<Integer>	Read-only	Tells the mon owner of the service. Minimum value = 0

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum value = 32
clmonview	<Integer>	Read-only	Tells the view id of the monitoring owner.
serviceipstr	<String>	Read-only	This field has been intorduced to show the dbs services ip.
oracleserverversion	<String>	Read-only	Oracle server version. Default value: 10G Possible values = 10G, 11G
nodefaultbindings	<String>	Read-only	to determine if the configuration will have default ssl CIPHER and ECC curve bindings. Default value: NO Possible values = YES, NO
monuserstatusmesg	<String>	Read-only	This field has been introduced to show user monitor failure reasons.
builtin	<String[]>	Read-only	. Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
feature	<String>	Read-only	The feature to be checked while applying this config.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- ENABLE
- DISABLE
- GET (ALL)
- GET
- COUNT
- RENAME

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of

creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

add

URL: http:// <netscaler-ip-address> /nitro/v1/config/service **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"service":{

<b>"name":<String_value>,

</b>"ip":<String_value>,

"servername":<String_value>,

<b>"servicetype":<String_value>,

</b><b>"port":<Integer_value>,

</b>"cleartextport":<Integer_value>,

"cachetype":<String_value>,

"maxclient":<Integer_value>,
```

```
"healthmonitor":<String_value>,

"maxreq":<Integer_value>,

"cacheable":<String_value>,

"cip":<String_value>,

"cipheader":<String_value>,

"usip":<String_value>,

"pathmonitor":<String_value>,

"pathmonitorindv":<String_value>,

"useproxyport":<String_value>,

"sp":<String_value>,

"rtspsessionidremap":<String_value>,

"clttimeout":<Integer_value>,

"svrtimeout":<Integer_value>,

"customserverid":<String_value>,

"serverid":<Integer_value>,

"cka":<String_value>,

"tcpb":<String_value>,

"cmp":<String_value>,

"maxbandwidth":<Integer_value>,

"accessdown":<String_value>,

"monthreshold":<Integer_value>,

"state":<String_value>,
```

```
"downstateflush":<String_value>,

"tcpprofilename":<String_value>,

"httpprofilename":<String_value>,

"contentinspectionprofilename":<String_value>,

"aigwprofilename":<String_value>,

"quicprofilename":<String_value>,

"hashid":<Integer_value>,

"comment":<String_value>,

"appflowlog":<String_value>,

"netprofile":<String_value>,

"td":<Integer_value>,

"processlocal":<String_value>,

"dnsprofilename":<String_value>,

"monconnectionclose":<String_value>,

"mcpprofilename":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

delete

URL: http:// <netscaler-ip-address> /nitro/v1/config/service/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

update

URL: http:// <netscaler-ip-address> /nitro/v1/config/service **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"service":{

<b>"name":<String_value>,

</b>"ipaddress":<String_value>,

"maxclient":<Integer_value>,

"maxreq":<Integer_value>,

"cacheable":<String_value>,

"cip":<String_value>,

"cipheader":<String_value>,

"usip":<String_value>,

"pathmonitor":<String_value>,

"pathmonitorindv":<String_value>,

"useproxyport":<String_value>,
```

```
"sp":<String_value>,

"rtspsessionidremap":<String_value>,

"healthmonitor":<String_value>,

"clttimeout":<Integer_value>,

"svrtimeout":<Integer_value>,

"customserverid":<String_value>,

"serverid":<Integer_value>,

"cka":<String_value>,

"tcpb":<String_value>,

"cmp":<String_value>,

"maxbandwidth":<Integer_value>,

"accessdown":<String_value>,

"monthreshold":<Integer_value>,

"weight":<Integer_value>,

"monitor_name_svc":<String_value>,

"downstateflush":<String_value>,

"tcpprofilename":<String_value>,

"httpprofilename":<String_value>,

"contentinspectionprofilename":<String_value>,

"quicprofilename":<String_value>,

"hashid":<Integer_value>,

"comment":<String_value>,
```

```
"appflowlog":<String_value>,

"netprofile":<String_value>,

"processlocal":<String_value>,

"dnsprofilename":<String_value>,

"monconnectionclose":<String_value>,

"mcpprofilename":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

unset

URL: http:// <netscaler-ip-address> /nitro/v1/config/service? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"service":{

<b>"name":<String_value>,

</b>"maxclient":true,

"maxreq":true,

"cacheable":true,

"cip":true,
```

```
"usip":true,
"pathmonitor":true,
"pathmonitorindv":true,
"useproxyport":true,
"sp":true,
"rtspsessionidremap":true,
"customserverid":true,
"serverid":true,
"cka":true,
"tcpb":true,
"cmp":true,
"maxbandwidth":true,
"accessdown":true,
"monthreshold":true,
"clttimeout":true,
"svrtimeout":true,
"tcpprofilename":true,
"httpprofilename":true,
"contentinspectionprofilename":true,
"hashid":true,
"appflowlog":true,
"netprofile":true,
```

```
"processlocal":true,

"dnsprofilename":true,

"quicprofilename":true,

"monconnectionclose":true,

"cipheader":true,

"healthmonitor":true,

"downstateflush":true,

"comment":true,

"mcpprofilename":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

enable

URL: http:// <netscaler-ip-address> /nitro/v1/config/service? **action=enable HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"service":{

<b>"name":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

disable

URL: http:// <netscaler-ip-address> /nitro/v1/config/service? **action=disable HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"service":{

<b>"name":<String_value>,

</b>"delay":<Integer_value>,

"graceful":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

rename

URL: http:// <netscaler-ip-address> /nitro/v1/config/service? **action=rename HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"service":{

<b>"name":<String_value>,

</b><b>"newname":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

get (all)

URL: http:// <netscaler-ip-address> /nitro/v1/config/service **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/service? **args=name: <String_value> ,all: <Boolean_value> ,Internal: <Boolean_value>**

Use this query-parameter to get service resources based on additional properties.

attrs http:// <netscaler-ip-address> /nitro/v1/config/service? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/service? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of service resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/service? **view=summary**

Use this query-parameter to get the summary output of service resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/service? **pagesize=#no;pageno=#no**

Use this query-parameter to get the service resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "service": [ {

name:<String_value>,all:<Boolean_value>,Internal:<Boolean_value>"numofconn
ections":<Integer_value>,

"servername":<String_value>,

"policyname":<String_value>,

"servicetype":<String_value>,

"serviceconftpye":<Boolean_value>,

"serviceconftype":<Boolean_value>,

"serviceconftype2":<String_value>,

"port":<Integer_value>,

"value":<String_value>,

"cleartextport":<Integer_value>,
```

```
"gslb":<String_value>,

"cachetype":<String_value>,

"maxclient":<Integer_value>,

"maxreq":<Integer_value>,

"cacheable":<String_value>,

"cip":<String_value>,

"cipheader":<String_value>,

"usip":<String_value>,

"pathmonitor":<String_value>,

"pathmonitorindv":<String_value>,

"useproxyport":<String_value>,

"dup_state":<String_value>,

"sp":<String_value>,

"rtspsessionidremap":<String_value>,

"clttimeout":<Integer_value>,

"svrtimeout":<Integer_value>,

"publicip":<String_value>,

"publicport":<Integer_value>,

"customserverid":<String_value>,

"serverid":<Integer_value>,

"cka":<String_value>,

"tcpb":<String_value>,
```

```
"processlocal":<String_value>,

"cmp":<String_value>,

"maxbandwidth":<Integer_value>,

"accessdown":<String_value>,

"svrstate":<String_value>,

"delay":<Integer_value>,

"ipaddress":<String_value>,

"monthreshold":<Integer_value>,

"monitor_state":<String_value>,

"monstatcode":<Integer_value>,

"lastresponse":<String_value>,

"responsetime":<Integer_value>,

"monstatparam1":<Integer_value>,

"monstatparam2":<Integer_value>,

"monstatparam3":<Integer_value>,

"downstateflush":<String_value>,

"statechangetimesec":<String_value>,

"statechangetimemsec":<Integer_value>,

"timesincelaststatechange":<Integer_value>,

"tickssincelaststatechange":<Integer_value>,

"stateupdatereason":<Integer_value>,

"clmonowner":<Integer_value>,
```

```
"clmonview":<Integer_value>,

"tcpprofilename":<String_value>,

"httpprofilename":<String_value>,

"contentinspectionprofilename":<String_value>,

"aigwprofilename":<String_value>,

"quicprofilename":<String_value>,

"hashid":<Integer_value>,

"graceful":<String_value>,

"comment":<String_value>,

"healthmonitor":<String_value>,

"appflowlog":<String_value>,

"netprofile":<String_value>,

"serviceipstr":<String_value>,

"weight":<Integer_value>,

"td":<Integer_value>,

"oracleserverversion":<String_value>,

"dnsprofilename":<String_value>,

"monconnectionclose":<String_value>,

"nodefaultbindings":<String_value>,

"monuserstatusmesg":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,
```

```
"mcpprofilename":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

get

URL: http:// <netscaler-ip-address> /nitro/v1/config/service/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/service/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/service/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of service resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "service": [ {

name:<String_value>,all:<Boolean_value>,Internal:<Boolean_value>"numofconn
ections":<Integer_value>,
```

```
"servername":<String_value>,

"policyname":<String_value>,

"servicetype":<String_value>,

"serviceconftpye":<Boolean_value>,

"serviceconftype":<Boolean_value>,

"serviceconftype2":<String_value>,

"port":<Integer_value>,

"value":<String_value>,

"cleartextport":<Integer_value>,

"gslb":<String_value>,

"cachetype":<String_value>,

"maxclient":<Integer_value>,

"maxreq":<Integer_value>,

"cacheable":<String_value>,

"cip":<String_value>,

"cipheader":<String_value>,

"usip":<String_value>,

"pathmonitor":<String_value>,

"pathmonitorindv":<String_value>,

"useproxyport":<String_value>,

"dup_state":<String_value>,

"sp":<String_value>,
```

```
"rtspsessionidremap":<String_value>,

"clttimeout":<Integer_value>,

"svrtimeout":<Integer_value>,

"publicip":<String_value>,

"publicport":<Integer_value>,

"customserverid":<String_value>,

"serverid":<Integer_value>,

"cka":<String_value>,

"tcpb":<String_value>,

"processlocal":<String_value>,

"cmp":<String_value>,

"maxbandwidth":<Integer_value>,

"accessdown":<String_value>,

"svrstate":<String_value>,

"delay":<Integer_value>,

"ipaddress":<String_value>,

"monthreshold":<Integer_value>,

"monitor_state":<String_value>,

"monstatcode":<Integer_value>,

"lastresponse":<String_value>,

"responsetime":<Integer_value>,

"monstatparam1":<Integer_value>,
```

```
"monstatparam2":<Integer_value>,

"monstatparam3":<Integer_value>,

"downstateflush":<String_value>,

"statechangetimesec":<String_value>,

"statechangetimemsec":<Integer_value>,

"timesincelaststatechange":<Integer_value>,

"tickssincelaststatechange":<Integer_value>,

"stateupdatereason":<Integer_value>,

"clmonowner":<Integer_value>,

"clmonview":<Integer_value>,

"tcpprofilename":<String_value>,

"httpprofilename":<String_value>,

"contentinspectionprofilename":<String_value>,

"aigwprofilename":<String_value>,

"quicprofilename":<String_value>,

"hashid":<Integer_value>,

"graceful":<String_value>,

"comment":<String_value>,

"healthmonitor":<String_value>,

"appflowlog":<String_value>,

"netprofile":<String_value>,

"serviceipstr":<String_value>,
```

```
"weight":<Integer_value>,

"td":<Integer_value>,

"oracleserverversion":<String_value>,

"dnsprofilename":<String_value>,

"monconnectionclose":<String_value>,

"nodefaultbindings":<String_value>,

"monuserstatusmesg":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"mcpprofilename":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

count

URL: http:// <netscaler-ip-address> /nitro/v1/config/service? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "service": [ { "__count": "#no"} ] }
```

cspolicy

Configuration for content-switching policy resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
policyname	<String>	Read-write	Name for the content switching policy. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at sign (@), equal sign (=), and hyphen (-) characters. Cannot be changed after a policy is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			marks (for example, "my policy" or 'my policy'). Minimum length = 1
rule	<String>	Read-write	Expression, or name of a named expression, against which traffic is evaluated. The following requirements apply only to the Citrix ADC CLI: * If the expression includes one or more spaces, enclose the entire expression in double quotation marks. * If the expression itself includes double quotation marks, escape the quotations by using the character. * Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			the double quotation marks.
action	<String>	Read-write	Content switching action that names the target load balancing virtual server to which the traffic is switched.
logaction	<String>	Read-write	The log action associated with the content switching policy.
newname	<String>	Read-write	The new name of the content switching policy. Minimum length = 1
vstype	<Integer>	Read-only	Virtual server type.
hits	<Integer>	Read-only	Total number of hits.
labelname	<String>	Read-only	Name of the label invoked.
labeltype	<String>	Read-only	The invocation type. Possible values = reqvserver, resvserver, policylabel
priority	<Integer>	Read-only	priority of bound policy.
activepolicy	<Boolean>	Read-only	Indicates whether policy is bound or not.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
boundto	<String>	Read-only	Location where policy is bound. Minimum length = 1
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- GET (ALL)
- GET
- COUNT
- RENAME

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.
- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

To do this, you must specify the username and password in the request header of the NITRO request as follows:

X-NITRO-USER: <username>

X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

add

URL: http:// <netscaler-ip-address> /nitro/v1/config/cspolicy **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"cspolicy":{

<b>"policyname":<String_value>,

</b><b>"rule":<String_value>,

</b>"action":<String_value>,

"logaction":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

delete

URL: http:// <netscaler-ip-address> /nitro/v1/config/cspolicy/ policyname_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

update

URL: http:// <netscaler-ip-address> /nitro/v1/config/cspolicy **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"cspolicy":{

<b>"policyname":<String_value>,

</b>"rule":<String_value>,

"action":<String_value>,

"logaction":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

unset

URL: http:// <netscaler-ip-address> /nitro/v1/config/cspolicy? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"cspolicy":{

<b>"policyname":<String_value>,

</b>"logaction":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

rename

URL: http:// <netscaler-ip-address> /nitro/v1/config/cspolicy? **action=rename HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"cspolicy":{

<b>"policyname":<String_value>,

</b><b>"newname":<String_value>
```

```
</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

get (all)

URL: http:// <netscaler-ip-address> /nitro/v1/config/cspolicy **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/cspolicy? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/cspolicy? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of cspolicy resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/cspolicy? **view=summary**

Use this query-parameter to get the summary output of cspolicy resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/cspolicy? **pagesize=#no;pageno=#no**

Use this query-parameter to get the cspolicy resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "cspolicy": [ {

"policyname":<String_value>,

"rule":<String_value>,

"action":<String_value>,

"vstype":<Integer_value>,

"hits":<Integer_value>,

"labelname":<String_value>,

"labeltype":<String_value>,

"target":<String_value>,

"priority":<Integer_value>,

"activepolicy":<Boolean_value>,

"logaction":<String_value>,

"boundto":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

get

URL: http:// <netscaler-ip-address> /nitro/v1/config/cspolicy/ policyname_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/cspolicy/ policyname_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/cspolicy/ policyname_value<String> ? **view=summary**

Use this query-parameter to get the summary output of cspolicy resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "cspolicy": [ {

"policyname":<String_value>,

"rule":<String_value>,

"action":<String_value>,

"vstype":<Integer_value>,

"hits":<Integer_value>,

"labelname":<String_value>,

"labeltype":<String_value>,
```

```
"target":<String_value>,

"priority":<Integer_value>,

"activepolicy":<Boolean_value>,

"logaction":<String_value>,

"boundto":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

count

URL: http:// <netscaler-ip-address> /nitro/v1/config/cspolicy? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "cspolicy": [ { "__count": "#no"} ] }
```

csvserver

Configuration for CS virtual server resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the content switching virtual server. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at sign (@), equal sign (=), and hyphen (-) characters. Cannot be changed after the CS virtual server is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, my server or my server). Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
td	<Integer>	Read-write	Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0. Minimum value = 0 Maximum value = 4094
servicetype	<String>	Read-write	Protocol used by the virtual server. Possible values = HTTP, SSL, TCP, FTP, RTSP, SSL_TCP, UDP, DNS, SIP_UDP, SIP_TCP, SIP_SSL, ANY, RADIUS, RDP, MYSQL, MSSQL, DIAMETER, SSL_DIAMETER, DNS_TCP, ORACLE, SMPP, PROXY, MONGO, MONGO_TLS, MQTT, MQTT_TLS, HTTP_QUIC, DOT, SSL_PROXY

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ipv46	<String>	Read-write	IP address of the content switching virtual server. Minimum length = 1
targettype	<String>	Read-write	Virtual server target type. Possible values = GSLB
dnsrecordtype	<String>	Read-write	. Default value: NSGSLB_IPV4 Possible values = A, AAAA, CNAME, NAPTR
persistenceid	<Integer>	Read-write	. Minimum value = 0 Maximum value = 65535
ippattern	<String>	Read-write	IP address pattern, in dotted decimal notation, for identifying packets to be accepted by the virtual server. The IP Mask parameter specifies which part of the destination IP address is matched against the pattern. Mutually exclusive with the IP Address parameter.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			For example, if the IP pattern assigned to the virtual server is 198.51.100.0 and the IP mask is 255.255.240.0 (a forward mask), the first 20 bits in the destination IP addresses are matched with the first 20 bits in the pattern. The virtual server accepts requests with IP addresses that range from 198.51.96.1 to 198.51.111.254. You can also use a pattern such as 0.0.2.2 and a mask such as 0.0.255.255 (a reverse mask). If a destination IP address matches more than one IP pattern, the pattern with the longest match is selected, and the associated virtual server processes the request. For example, if the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			virtual servers, vs1 and vs2, have the same IP pattern, 0.0.100.128, but different IP masks of 0.0.255.255 and 0.0.224.255, a destination IP address of 198.51.100.128 has the longest match with the IP pattern of vs1. If a destination IP address matches two or more virtual servers to the same extent, the request is processed by the virtual server whose port number matches the port number in the request.
ipmask	<String>	Read-write	IP mask, in dotted decimal notation, for the IP Pattern parameter. Can have leading or trailing non-zero octets (for example, 255.255.240.0 or 0.0.255.255). Accordingly, the mask specifies whether the first n bits or the last n bits

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			of the destination IP address in a client request are to be matched with the corresponding bits in the IP pattern. The former is called a forward mask. The latter is called a reverse mask.
range	<Integer>	Read-write	Number of consecutive IP addresses, starting with the address specified by the IP Address parameter, to include in a range of addresses assigned to this virtual server. Default value: 1 Minimum value = 1 Maximum value = 254
port	<Integer>	Read-write	Port number for content switching virtual server. Minimum value = 1 Range 1 - 65535 * in CLI is represented as 65535 in NITRO API

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ipset	<String>	Read-write	The list of IPv4/IPv6 addresses bound to ipset would form a part of listening service on the current cs vserver. Minimum length = 1
state	<String>	Read-write	Initial state of the load balancing virtual server. Default value: ENABLED Possible values = ENABLED, DISABLED
stateupdate	<String>	Read-write	Enable state updates for a specific content switching virtual server. By default, the Content Switching virtual server is always UP, regardless of the state of the Load Balancing virtual servers bound to it. This parameter interacts with the global setting as follows: Global Level | Vserver Level | Result

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			ENABLED ENABLED ENABLED ENABLED DISABLED ENABLED DISABLED ENABLED ENABLED DISABLED DISABLED DISABLED If you want to enable state updates for only some content switching virtual servers, be sure to disable the state update parameter. Default value: DISABLED Possible values = ENABLED, DISABLED, UPDATEONBACKENDUPDATE
cacheable	<String>	Read-write	Use this option to specify whether a virtual server, used for load balancing or content switching,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			routes requests to the cache redirection virtual server before sending it to the configured servers. Default value: NO Possible values = YES, NO
redirecturl	<String>	Read-write	URL to which traffic is redirected if the virtual server becomes unavailable. The service type of the virtual server should be either HTTP or SSL. Caution: Make sure that the domain in the URL does not match the domain specified for a content switching policy. If it does, requests are continuously redirected to the unavailable virtual server. Minimum length = 1
clttimeout	<Integer>	Read-write	Idle time, in seconds, after which the client connection is terminated. The default values are:

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			180 seconds for HTTP/SSL-based services. 9000 seconds for other TCP-based services. 120 seconds for DNS-based services. 120 seconds for other UDP-based services. Minimum value = 0 Maximum value = 31536000
precedence	<String>	Read-write	Type of precedence to use for both RULE-based and URL-based policies on the content switching virtual server. With the default (RULE) setting, incoming requests are evaluated against the rule-based content switching policies. If none of the rules match, the URL in the request is evaluated against the URL-based

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			content switching policies. Default value: RULE Possible values = RULE, URL
casesensitive	<String>	Read-write	Consider case in URLs (for policies that use URLs instead of RULES). For example, with the ON setting, the URLs /a/1.html and /A/1.HTML are treated differently and can have different targets (set by content switching policies). With the OFF setting, /a/1.html and /A/1.HTML are switched to the same target. Default value: ON Possible values = ON, OFF
somethod	<String>	Read-write	Type of spillover used to divert traffic to the backup virtual server when the primary virtual server reaches the spillover threshold. Connection spillover is based on the number of connections.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Bandwidth spillover is based on the total Kbps of incoming and outgoing traffic. Possible values = CONNECTION, DYNAMICCONNECTION, BANDWIDTH, HEALTH, LLMQUOTA, NONE
sopersistence	<String>	Read-write	Maintain source-IP based persistence on primary and backup virtual servers. Default value: DISABLED Possible values = ENABLED, DISABLED
sopersistencetimeout	<Integer>	Read-write	Time-out value, in minutes, for spillover persistence. Default value: 2 Minimum value = 2 Maximum value = 1440
sothreshold	<Integer>	Read-write	Depending on the spillover method, the maximum number of connections or the maximum total bandwidth (Kbps)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			that a virtual server can handle before spillover occurs. Minimum value = 1 Maximum value = 4294967287
sobackupaction	<String>	Read-write	Action to be performed if spillover is to take effect, but no backup chain to spillover is usable or exists. Possible values = DROP, ACCEPT, REDIRECT
redirectportrewrite	<String>	Read-write	State of port rewrite while performing HTTP redirect. Default value: DISABLED Possible values = ENABLED, DISABLED
downstateflush	<String>	Read-write	Flush all active transactions associated with a virtual server whose state transitions from UP to DOWN. Do not enable this option for applications that must complete their transactions.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: ENABLED Possible values = ENABLED, DISABLED
backupvserver	<String>	Read-write	Name of the backup virtual server that you are configuring. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at sign (@), equal sign (=), and hyphen (-) characters. Can be changed after the backup virtual server is created. You can assign a different backup virtual server or rename the existing virtual server. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			single quotation marks. Minimum length = 1
disableprimaryondown	<String>	Read-write	Continue forwarding the traffic to backup virtual server even after the primary server comes UP from the DOWN state. Default value: DISABLED Possible values = ENABLED, DISABLED
insertvserveripport	<String>	Read-write	Insert the virtual server's VIP address and port number in the request header. Available values function as follows: VIPADDR - Header contains the vserver's IP address and port number without any translation. OFF - The virtual IP and port header insertion option is disabled. V6TOV4MAPPING - Header contains the mapped IPv4

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			address corresponding to the IPv6 address of the vserver and the port number. An IPv6 address can be mapped to a user-specified IPv4 address using the set ns ip6 command. Possible values = OFF, VIPADDR, V6TOV4MAPPING
vipheader	<String>	Read-write	Name of virtual server IP and port header, for use with the VServer IP Port Insertion parameter. Minimum length = 1
rtspnat	<String>	Read-write	Enable network address translation (NAT) for real-time streaming protocol (RTSP) connections. Default value: OFF Possible values = ON, OFF
authenticationhost	<String>	Read-write	FQDN of the authentication virtual server. The service type of the virtual server should be either HTTP or SSL.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum length = 3 Maximum length = 252
authentication	<String>	Read-write	Authenticate users who request a connection to the content switching virtual server. Default value: OFF Possible values = ON, OFF
listenpolicy	<String>	Read-write	String specifying the listen policy for the content switching virtual server. Can be either the name of an existing expression or an in-line expression. Default value: "NONE"
listenpriority	<Integer>	Read-write	Integer specifying the priority of the listen policy. A higher number specifies a lower priority. If a request matches the listen policies of more than one virtual server the virtual server whose listen policy has the highest priority (the lowest priority

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			number) accepts the request. Default value: 101 Minimum value = 0 Maximum value = 100
authn401	<String>	Read-write	Enable HTTP 401-response based authentication. Default value: OFF Possible values = ON, OFF
authnvsname	<String>	Read-write	Name of authentication virtual server that authenticates the incoming user requests to this content switching virtual server. . Minimum length = 1 Maximum length = 252
push	<String>	Read-write	Process traffic with the push virtual server that is bound to this content switching virtual server (specified by the Push VServer parameter). The service type of the push virtual server

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			should be either HTTP or SSL. Default value: DISABLED Possible values = ENABLED, DISABLED
pushvserver	<String>	Read-write	Name of the load balancing virtual server, of type PUSH or SSL_PUSH, to which the server pushes updates received on the client-facing load balancing virtual server. Minimum length = 1
pushlabel	<String>	Read-write	Expression for extracting the label from the response received from server. This string can be either an existing rule name or an inline expression. The service type of the virtual server should be either HTTP or SSL. Default value: "none"
pushmulticlients	<String>	Read-write	Allow multiple Web 2.0 connections from the same client to connect to the virtual

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			server and expect updates. Default value: NO Possible values = YES, NO
tcpprofilename	<String>	Read-write	Name of the TCP profile containing TCP configuration settings for the virtual server. Minimum length = 1 Maximum length = 127
httpprofilename	<String>	Read-write	Name of the HTTP profile containing HTTP configuration settings for the virtual server. The service type of the virtual server should be either HTTP or SSL. Minimum length = 1 Maximum length = 127
dbprofilename	<String>	Read-write	Name of the DB profile. Minimum length = 1 Maximum length = 127
oracleserverversion	<String>	Read-write	Oracle server version.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: 10G Possible values = 10G, 11G
comment	<String>	Read-write	Information about this virtual server.
mssqlserverversion	<String>	Read-write	The version of the MSSQL server. Default value: 2008R2 Possible values = 70, 2000, 2000SP1, 2005, 2008, 2008R2, 2012, 2014
l2conn	<String>	Read-write	Use L2 Parameters to identify a connection. Possible values = ON, OFF
mysqlprotocolversion	<Integer>	Read-write	The protocol version returned by the mysql vserver. Default value: 10
mysqlserverversion	<String>	Read-write	The server version string returned by the mysql vserver. Minimum length = 1 Maximum length = 31

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
mysqlcharacterset	<Integer>	Read-write	The character set returned by the mysql vserver. Default value: 8
mysqlservercapabilities	<Integer>	Read-write	The server capabilities returned by the mysql vserver. Default value: 41613
appflowlog	<String>	Read-write	Enable logging appflow flow information. Default value: ENABLED Possible values = ENABLED, DISABLED
netprofile	<String>	Read-write	The name of the network profile. Minimum length = 1 Maximum length = 127
icmpvsrresponse	<String>	Read-write	Can be active or passive. Default value: PASSIVE Possible values = PASSIVE, ACTIVE
rhistate	<String>	Read-write	A host route is injected according to the setting on the virtual servers

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			* If set to PASSIVE on all the virtual servers that share the IP address, the appliance always injects the hostroute. * If set to ACTIVE on all the virtual servers that share the IP address, the appliance injects even if one virtual server is UP. * If set to ACTIVE on some virtual servers and PASSIVE on the others, the appliance, injects even if one virtual server set to ACTIVE is UP. Default value: PASSIVE Possible values = PASSIVE, ACTIVE
authnprofile	<String>	Read-write	Name of the authentication profile to be used when authentication is turned on.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
dnsprofilename	<String>	Read-write	Name of the DNS profile to be associated with the VServer. DNS profile properties will applied to the transactions processed by a VServer. This parameter is valid only for DNS and DNS-TCP VServers. Minimum length = 1 Maximum length = 127
dtls	<String>	Read-write	This option starts/stops the dtls service on the vserver. Default value: OFF Possible values = ON, OFF
persistencetype	<String>	Read-write	Type of persistence for the virtual server. Available settings function as follows: * SOURCEIP - Connections from the same client IP address belong to the same persistence session. * COOKIEINSERT - Connections that have the same

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			HTTP Cookie, inserted by a Set-Cookie directive from a server, belong to the same persistence session. * SSLSESSION - Connections that have the same SSL Session ID belong to the same persistence session. Possible values = SOURCEIP, COOKIEINSERT, SSLSESSION, NONE
persistmask	<String>	Read-write	Persistence mask for IP based persistence types, for IPv4 virtual servers. Minimum length = 1
v6persistmasklen	<Integer>	Read-write	Persistence mask for IP based persistence types, for IPv6 virtual servers. Default value: 128 Minimum value = 1 Maximum value = 128

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
timeout	<Integer>	Read-write	Time period for which a persistence session is in effect. Default value: 2 Minimum value = 0 Maximum value = 1440
cookiename	<String>	Read-write	Use this parameter to specify the cookie name for COOKIE peristence type. It specifies the name of cookie with a maximum of 32 characters. If not specified, cookie name is internally generated.
persistencebackup	<String>	Read-write	Backup persistence type for the virtual server. Becomes operational if the primary persistence mechanism fails. Possible values = SOURCEIP, NONE
backuppersistencetimeout	<Integer>	Read-write	Time period for which backup persistence is in effect. Default value: 2 Minimum value = 2

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum value = 1440
tcpprobeport	<Integer>	Read-write	Port number for external TCP probe. NetScaler provides support for external TCP health check of the vserver status over the selected port. This option is only supported for vservers assigned with an IPAddress or ipset. Minimum value = 1 Range 1 - 65535 * in CLI is represented as 65535 in NITRO API
probeprotocol	<String>	Read-write	Citrix ADC provides support for external health check of the vserver status. Select HTTP or TCP probes for healthcheck. Possible values = TCP, HTTP
probesuccessresponsecode	<String>	Read-write	HTTP code to return in SUCCESS case. Default value: "200 OK"

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum length = 1 Maximum length = 64
probeport	<Integer>	Read-write	Citrix ADC provides support for external health check of the vserver status. Select port for HTTP/ TCP monitring. Default value: 0 Range 1 - 65535 * in CLI is represented as 65535 in NITRO API
quicprofilename	<String>	Read-write	Name of QUIC profile which will be attached to the Content Switching VServer. Minimum length = 1 Maximum length = 255
redirectfromport	<Integer>	Read-write	Port number for the virtual server, from which we absorb the traffic for http redirect. Minimum value = 1 Range 1 - 65535 * in CLI is represented as

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			65535 in NITRO API
mcpprofilename	<String>	Read-write	Name of the MCP profile to attach to this cs vserver. Enables MCP protocol processing.
dnsoverhttps	<String>	Read-write	This option is used to enable/disable DNS over HTTPS (DoH) processing. Default value: DISABLED Possible values = ENABLED, DISABLED
httpsredirecturl	<String>	Read-write	URL to which all HTTP traffic received on the port specified in the -redirectFromPort parameter is redirected.
apiprofile	<String>	Read-write	The API profile where one or more API specs are bounded to. Minimum length = 1
wasmmodule	<String>	Read-write	Name of the WASM module to assign to this virtual server.
aigwprofilename	<String>	Read-write	Name of the AIGW frontend profile. For the content switching

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			vserver to function as AI gateway, this parameter must be set. Once this parameter is set using add cs vserver, it cannot be unset. Minimum length = 1 Maximum length = 255
domainname	<String>	Read-write	Domain name for which to change the time to live (TTL) and/or backup service IP address. Minimum length = 1
ttl	<Integer>	Read-write	. Minimum value = 1
backupip	<String>	Read-write	. Minimum length = 1
cookiedomain	<String>	Read-write	. Minimum length = 1
cookietimeout	<Integer>	Read-write	. Minimum value = 0 Maximum value = 1440
sitedomainttl	<Integer>	Read-write	. Minimum value = 1
newname	<String>	Read-write	New name for the virtual server. Must begin with an ASCII alphanumeric or

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at sign (@), equal sign (=), and hyphen (-) characters. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my name" or 'my name'). Minimum length = 1
ip	<String>	Read-only	The IP address of the virtual server.
value	<String>	Read-only	The ssl card status for the transparent ssl cs vserver. Possible values = Certkey/ Certkeybundle/Vault not bound/Cert-store not usable, SSL feature disabled

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ngname	<String>	Read-only	Nodegroup devno to which this csvserver belongs to.
type	<String>	Read-only	Virtual server type. Possible values = CONTENT, ADDRESS
curstate	<String>	Read-only	The state of the cs vserver. Possible values = UP, DOWN, UNKNOWN, BUSY, OUT OF SERVICE, GOING OUT OF SERVICE, DOWN WHEN GOING OUT OF SERVICE, NS_EMPTY_STR, Unknown, DISABLED
status	<Integer>	Read-only	Status.
cachetype	<String>	Read-only	Cache type. Possible values = TRANSPARENT, REVERSE, FORWARD
redirect	<String>	Read-only	Redirect URL string. Possible values = CACHE, POLICY, ORIGIN
homepage	<String>	Read-only	Home page.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
dnsvservername	<String>	Read-only	DNS vserver name.
domain	<String>	Read-only	Domain.
servicename	<String>	Read-only	Service name.
weight	<Integer>	Read-only	Weight for this service.
cachevserver	<String>	Read-only	Cache vserver name.
targetvserver	<String>	Read-only	target vserver name.
url	<String>	Read-only	URL string.
bindpoint	<String>	Read-only	The bindpoint to which the policy is bound. Possible values = REQUEST, RESPONSE, ICA_REQUEST, OTHERTCP_REQUEST, MQTT_JUMBO_REQ
gt2gb	<String>	Read-only	This argument has no effect. Default value: DISABLED Possible values = ENABLED, DISABLED
statechangetimesec	<String>	Read-only	Time when last state change happened. Seconds part.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
statechangetimemsec	<Integer>	Read-only	Time at which last state change happened. Milliseconds part.
tickssincelaststatechange	<Integer>	Read-only	Time in 10 millisecond ticks since the last state change.
ruletype	<Integer>	Read-only	Rule type.
lbvserver	<String>	Read-only	Name of the default lb vserver bound. Use this param for Default binding only. For Example: bind cs vserver cs1 -lbvserver lb1. Minimum length = 1
targetlbvserver	<String>	Read-only	target vserver name.
nodefaultbindings	<String>	Read-only	to determine if the configuration will have default ssl CIPHER and ECC curve bindings. Default value: NO Possible values = YES, NO
version	<Integer>	Read-only	Cookie version.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- ENABLE
- DISABLE
- GET (ALL)
- GET
- COUNT
- RENAME

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

add

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"csvserver":{

<b>"name":<String_value>,

</b>"td":<Integer_value>,

<b>"servicetype":<String_value>,

</b>"ipv46":<String_value>,

"targettype":<String_value>,

"dnsrecordtype":<String_value>,

"persistenceid":<Integer_value>,

"ippattern":<String_value>,

"ipmask":<String_value>,

"range":<Integer_value>,

"port":<Integer_value>,

"ipset":<String_value>,

"state":<String_value>,

"stateupdate":<String_value>,
```

```
"cacheable":<String_value>,

"redirecturl":<String_value>,

"clttimeout":<Integer_value>,

"precedence":<String_value>,

"casesensitive":<String_value>,

"somethod":<String_value>,

"sopersistence":<String_value>,

"sopersistencetimeout":<Integer_value>,

"sothreshold":<Integer_value>,

"sobackupaction":<String_value>,

"redirectportrewrite":<String_value>,

"downstateflush":<String_value>,

"backupvserver":<String_value>,

"disableprimaryondown":<String_value>,

"insertvserveripport":<String_value>,

"vipheader":<String_value>,

"rtspnat":<String_value>,

"authenticationhost":<String_value>,

"authentication":<String_value>,

"listenpolicy":<String_value>,

"listenpriority":<Integer_value>,

"authn401":<String_value>,
```

```
"authnvsname":<String_value>,

"push":<String_value>,

"pushvserver":<String_value>,

"pushlabel":<String_value>,

"pushmulticlients":<String_value>,

"tcpprofilename":<String_value>,

"httpprofilename":<String_value>,

"dbprofilename":<String_value>,

"oracleserverversion":<String_value>,

"comment":<String_value>,

"mssqlserverversion":<String_value>,

"l2conn":<String_value>,

"mysqlprotocolversion":<Integer_value>,

"mysqlserverversion":<String_value>,

"mysqlcharacterset":<Integer_value>,

"mysqlservercapabilities":<Integer_value>,

"appflowlog":<String_value>,

"netprofile":<String_value>,

"icmpvsrresponse":<String_value>,

"rhistate":<String_value>,

"authnprofile":<String_value>,

"dnsprofilename":<String_value>,
```

```
"dtls":<String_value>,

"persistencetype":<String_value>,

"persistmask":<String_value>,

"v6persistmasklen":<Integer_value>,

"timeout":<Integer_value>,

"cookiename":<String_value>,

"persistencebackup":<String_value>,

"backuppersistencetimeout":<Integer_value>,

"tcpprobeport":<Integer_value>,

"probeprotocol":<String_value>,

"probesuccessresponsecode":<String_value>,

"probeport":<Integer_value>,

"quicprofilename":<String_value>,

"redirectfromport":<Integer_value>,

"mcpprofilename":<String_value>,

"dnsoverhttps":<String_value>,

"httpsredirecturl":<String_value>,

"apiprofile":<String_value>,

"wasmmodule":<String_value>,

"aigwprofilename":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

delete

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

update

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"csvserver":{

<b>"name":<String_value>,

</b>"ipv46":<String_value>,

"ipset":<String_value>,

"ippattern":<String_value>,

"ipmask":<String_value>,
```

```
"stateupdate":<String_value>,

"precedence":<String_value>,

"casesensitive":<String_value>,

"backupvserver":<String_value>,

"redirecturl":<String_value>,

"cacheable":<String_value>,

"clttimeout":<Integer_value>,

"somethod":<String_value>,

"sopersistence":<String_value>,

"sopersistencetimeout":<Integer_value>,

"sothreshold":<Integer_value>,

"sobackupaction":<String_value>,

"redirectportrewrite":<String_value>,

"downstateflush":<String_value>,

"disableprimaryondown":<String_value>,

"insertvserveripport":<String_value>,

"vipheader":<String_value>,

"rtspnat":<String_value>,

"authenticationhost":<String_value>,

"authentication":<String_value>,

"listenpolicy":<String_value>,

"listenpriority":<Integer_value>,
```

```
"authn401":<String_value>,

"authnvsname":<String_value>,

"push":<String_value>,

"pushvserver":<String_value>,

"pushlabel":<String_value>,

"pushmulticlients":<String_value>,

"tcpprofilename":<String_value>,

"httpprofilename":<String_value>,

"dbprofilename":<String_value>,

"mcpprofilename":<String_value>,

"comment":<String_value>,

"l2conn":<String_value>,

"mssqlserverversion":<String_value>,

"mysqlprotocolversion":<Integer_value>,

"oracleserverversion":<String_value>,

"mysqlserverversion":<String_value>,

"mysqlcharacterset":<Integer_value>,

"mysqlservercapabilities":<Integer_value>,

"appflowlog":<String_value>,

"netprofile":<String_value>,

"authnprofile":<String_value>,

"icmpvsrresponse":<String_value>,
```

```
"rhistate":<String_value>,

"dnsprofilename":<String_value>,

"dnsrecordtype":<String_value>,

"persistenceid":<Integer_value>,

"domainname":<String_value>,

"ttl":<Integer_value>,

"backupip":<String_value>,

"cookiedomain":<String_value>,

"cookietimeout":<Integer_value>,

"sitedomainttl":<Integer_value>,

"dtls":<String_value>,

"persistencetype":<String_value>,

"persistmask":<String_value>,

"v6persistmasklen":<Integer_value>,

"timeout":<Integer_value>,

"cookiename":<String_value>,

"persistencebackup":<String_value>,

"backuppersistencetimeout":<Integer_value>,

"tcpprobeport":<Integer_value>,

"probeprotocol":<String_value>,

"probesuccessresponsecode":<String_value>,

"probeport":<Integer_value>,
```

```
"quicprofilename":<String_value>,

"redirectfromport":<Integer_value>,

"httpsredirecturl":<String_value>,

"dnsoverhttps":<String_value>,

"apiprofile":<String_value>,

"wasmmodule":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

unset

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"csvserver":{

<b>"name":<String_value>,

</b>"casesensitive":true,

"backupvserver":true,

"clttimeout":true,
```

```
"redirecturl":true,

"authn401":true,

"authentication":true,

"authenticationhost":true,

"authnvsname":true,

"pushvserver":true,

"pushlabel":true,

"tcpprofilename":true,

"httpprofilename":true,

"dbprofilename":true,

"l2conn":true,

"mysqlprotocolversion":true,

"mysqlserverversion":true,

"mysqlcharacterset":true,

"mysqlservercapabilities":true,

"appflowlog":true,

"netprofile":true,

"icmpvsrresponse":true,

"authnprofile":true,

"sothreshold":true,

"dnsprofilename":true,

"tcpprobeport":true,
```

```
"probeprotocol":true,

"quicprofilename":true,

"redirectfromport":true,

"httpsredirecturl":true,

"apiprofile":true,

"dnsoverhttps":true,

"wasmmodule":true,

"ipset":true,

"stateupdate":true,

"precedence":true,

"cacheable":true,

"somethod":true,

"sopersistence":true,

"sopersistencetimeout":true,

"sobackupaction":true,

"redirectportrewrite":true,

"downstateflush":true,

"disableprimaryondown":true,

"insertvserveripport":true,

"vipheader":true,

"rtspnat":true,

"listenpolicy":true,
```

```
"listenpriority":true,

"push":true,

"pushmulticlients":true,

"mcpprofilename":true,

"comment":true,

"mssqlserverversion":true,

"oracleserverversion":true,

"rhistate":true,

"dnsrecordtype":true,

"persistenceid":true,

"dtls":true,

"persistencetype":true,

"persistmask":true,

"v6persistmasklen":true,

"timeout":true,

"cookiename":true,

"persistencebackup":true,

"backuppersistencetimeout":true,

"probesuccessresponsecode":true

}}
```


Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

enable

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver? **action=enable HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"csvserver":{

<b>"name":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

disable

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver? **action=disable HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"csvserver":{

<b>"name":<String_value>
```

```
</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

rename

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver? **action=rename HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"csvserver":{

<b>"name":<String_value>,

</b><b>"newname":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

get (all)

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/csvserver? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/csvserver? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of csvserver resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/csvserver? **view=summary**

Use this query-parameter to get the summary output of csvserver resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/csvserver? **pagesize=#no;pageno=#no**

Use this query-parameter to get the csvserver resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "csvserver": [ {

"name":<String_value>,

"insertvserveripport":<String_value>,

"vipheader":<String_value>,

"ip":<String_value>,
```

```
"td":<Integer_value>,

"ipv46":<String_value>,

"ippattern":<String_value>,

"ipmask":<String_value>,

"value":<String_value>,

"port":<Integer_value>,

"ipset":<String_value>,

"range":<Integer_value>,

"servicetype":<String_value>,

"ngname":<String_value>,

"type":<String_value>,

"curstate":<String_value>,

"stateupdate":<String_value>,

"status":<Integer_value>,

"cachetype":<String_value>,

"redirect":<String_value>,

"precedence":<String_value>,

"redirecturl":<String_value>,

"authentication":<String_value>,

"authn401":<String_value>,

"authnvsname":<String_value>,

"casesensitive":<String_value>,
```

```
"homepage":<String_value>,

"dnsvservername":<String_value>,

"domain":<String_value>,

"servicename":<String_value>,

"weight":<Integer_value>,

"cachevserver":<String_value>,

"targetvserver":<String_value>,

"backupvserver":<String_value>,

"clttimeout":<Integer_value>,

"listenpolicy":<String_value>,

"listenpriority":<Integer_value>,

"somethod":<String_value>,

"sopersistence":<String_value>,

"sopersistencetimeout":<Integer_value>,

"sothreshold":<Integer_value>,

"sobackupaction":<String_value>,

"cacheable":<String_value>,

"url":<String_value>,

"redirectportrewrite":<String_value>,

"downstateflush":<String_value>,

"disableprimaryondown":<String_value>,

"bindpoint":<String_value>,
```

```
"gt2gb":<String_value>,

"statechangetimesec":<String_value>,

"statechangetimemsec":<Integer_value>,

"tickssincelaststatechange":<Integer_value>,

"rtspnat":<String_value>,

"authenticationhost":<String_value>,

"push":<String_value>,

"pushvserver":<String_value>,

"pushlabel":<String_value>,

"pushmulticlients":<String_value>,

"tcpprofilename":<String_value>,

"httpprofilename":<String_value>,

"dbprofilename":<String_value>,

"comment":<String_value>,

"oracleserverversion":<String_value>,

"mssqlserverversion":<String_value>,

"l2conn":<String_value>,

"ruletype":<Integer_value>,

"mysqlprotocolversion":<Integer_value>,

"mysqlserverversion":<String_value>,

"mysqlcharacterset":<Integer_value>,

"mysqlservercapabilities":<Integer_value>,
```

```
"appflowlog":<String_value>,

"netprofile":<String_value>,

"icmpvsrresponse":<String_value>,

"rhistate":<String_value>,

"lbvserver":<String_value>,

"targetlbvserver":<String_value>,

"authnprofile":<String_value>,

"dnsprofilename":<String_value>,

"targettype":<String_value>,

"domainname":<String_value>,

"ttl":<Integer_value>,

"backupip":<String_value>,

"cookiedomain":<String_value>,

"cookietimeout":<Integer_value>,

"sitedomainttl":<Integer_value>,

"dnsrecordtype":<String_value>,

"persistenceid":<Integer_value>,

"dtls":<String_value>,

"nodefaultbindings":<String_value>,

"persistencetype":<String_value>,

"persistmask":<String_value>,

"v6persistmasklen":<Integer_value>,
```

```
"timeout":<Integer_value>,

"cookiename":<String_value>,

"version":<Integer_value>,

"persistencebackup":<String_value>,

"backuppersistencetimeout":<Integer_value>,

"tcpprobeport":<Integer_value>,

"probeprotocol":<String_value>,

"probeport":<Integer_value>,

"probesuccessresponsecode":<String_value>,

"quicprofilename":<String_value>,

"redirectfromport":<Integer_value>,

"httpsredirecturl":<String_value>,

"apiprofile":<String_value>,

"mcpprofilename":<String_value>,

"dnsoverhttps":<String_value>,

"wasmmodule":<String_value>,

"aigwprofilename":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

get

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/csvserver/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/csvserver/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of csvserver resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "csvserver": [ {

"name":<String_value>,

"insertvserveripport":<String_value>,

"vipheader":<String_value>,

"ip":<String_value>,
```

```
"td":<Integer_value>,

"ipv46":<String_value>,

"ippattern":<String_value>,

"ipmask":<String_value>,

"value":<String_value>,

"port":<Integer_value>,

"ipset":<String_value>,

"range":<Integer_value>,

"servicetype":<String_value>,

"ngname":<String_value>,

"type":<String_value>,

"curstate":<String_value>,

"stateupdate":<String_value>,

"status":<Integer_value>,

"cachetype":<String_value>,

"redirect":<String_value>,

"precedence":<String_value>,

"redirecturl":<String_value>,

"authentication":<String_value>,

"authn401":<String_value>,

"authnvsname":<String_value>,

"casesensitive":<String_value>,
```

```
"homepage":<String_value>,

"dnsvservername":<String_value>,

"domain":<String_value>,

"servicename":<String_value>,

"weight":<Integer_value>,

"cachevserver":<String_value>,

"targetvserver":<String_value>,

"backupvserver":<String_value>,

"clttimeout":<Integer_value>,

"listenpolicy":<String_value>,

"listenpriority":<Integer_value>,

"somethod":<String_value>,

"sopersistence":<String_value>,

"sopersistencetimeout":<Integer_value>,

"sothreshold":<Integer_value>,

"sobackupaction":<String_value>,

"cacheable":<String_value>,

"url":<String_value>,

"redirectportrewrite":<String_value>,

"downstateflush":<String_value>,

"disableprimaryondown":<String_value>,

"bindpoint":<String_value>,
```

```
"gt2gb":<String_value>,

"statechangetimesec":<String_value>,

"statechangetimemsec":<Integer_value>,

"tickssincelaststatechange":<Integer_value>,

"rtspnat":<String_value>,

"authenticationhost":<String_value>,

"push":<String_value>,

"pushvserver":<String_value>,

"pushlabel":<String_value>,

"pushmulticlients":<String_value>,

"tcpprofilename":<String_value>,

"httpprofilename":<String_value>,

"dbprofilename":<String_value>,

"comment":<String_value>,

"oracleserverversion":<String_value>,

"mssqlserverversion":<String_value>,

"l2conn":<String_value>,

"ruletype":<Integer_value>,

"mysqlprotocolversion":<Integer_value>,

"mysqlserverversion":<String_value>,

"mysqlcharacterset":<Integer_value>,

"mysqlservercapabilities":<Integer_value>,
```

```
"appflowlog":<String_value>,

"netprofile":<String_value>,

"icmpvsrresponse":<String_value>,

"rhistate":<String_value>,

"lbvserver":<String_value>,

"targetlbvserver":<String_value>,

"authnprofile":<String_value>,

"dnsprofilename":<String_value>,

"targettype":<String_value>,

"domainname":<String_value>,

"ttl":<Integer_value>,

"backupip":<String_value>,

"cookiedomain":<String_value>,

"cookietimeout":<Integer_value>,

"sitedomainttl":<Integer_value>,

"dnsrecordtype":<String_value>,

"persistenceid":<Integer_value>,

"dtls":<String_value>,

"nodefaultbindings":<String_value>,

"persistencetype":<String_value>,

"persistmask":<String_value>,

"v6persistmasklen":<Integer_value>,
```

```
"timeout":<Integer_value>,

"cookiename":<String_value>,

"version":<Integer_value>,

"persistencebackup":<String_value>,

"backuppersistencetimeout":<Integer_value>,

"tcpprobeport":<Integer_value>,

"probeprotocol":<String_value>,

"probeport":<Integer_value>,

"probesuccessresponsecode":<String_value>,

"quicprofilename":<String_value>,

"redirectfromport":<Integer_value>,

"httpsredirecturl":<String_value>,

"apiprofile":<String_value>,

"mcpprofilename":<String_value>,

"dnsoverhttps":<String_value>,

"wasmmodule":<String_value>,

"aigwprofilename":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

count

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "csvserver": [ { "__count": "#no"} ] }
```

csvserver_cspolicy_binding

Binding object showing the cspolicy that can be bound to csvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
targetlbvserver	<String>	Read-write	target vserver name.
policyname	<String>	Read-write	Policies bound to this vserver.
gotopriorityexpression	<String>	Read-write	Expression specifying the priority of the next policy which will get evaluated if the current policy rule evaluates to TRUE.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
invoke	<Boolean>	Read-write	Invoke flag.
name	<String>	Read-write	Name of the content switching virtual server to which the content switching policy applies. Minimum length = 1
bindpoint	<String>	Read-write	The bindpoint to which the policy is bound. Possible values = REQUEST, RESPONSE, ICA_REQUEST, OTHERTCP_REQUEST, MQTT_JUMBO_REQ
labeltype	<String>	Read-write	The invocation type. Possible values = reqvserver, resvserver, policylabel
priority	<Integer>	Read-write	Priority for the policy.
labelname	<String>	Read-write	Name of the label invoked.
cookieipport	<String>	Read-only	Vserver id of the lb vserver that is inserted into the set-cookie HTTP header.
hits	<Integer>	Read-only	Number of hits.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
pipolicyhits	<Integer>	Read-only	Number of hits.
vserverid	<String>	Read-only	Vserver Id of vserver.
rule	<String>	Read-only	Rule.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

Note: In such cases, make sure that the request header DOES not include the following:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

add

URL: http:// <netscaler-ip-address /nitro/v1/config/csvserver_cspolicy_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"csvserver_cspolicy_binding":{

<b>"name":<String_value>,

</b>"policyname":<String_value>,

"targetlbvserver":<String_value>,

"priority":<Integer_value>,

"gotopriorityexpression":<String_value>,

"bindpoint":<String_value>,

"invoke":<Boolean_value>,

"labeltype":<String_value>,

"labelname":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

delete

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver_cspolicy_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ csvserver_cspolicy_binding/ name_value<String> ? **args=policyname: <String_value> ,bindpoint: <String_value> ,priority: <Integer_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

get

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver_cspolicy_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ csvserver_cspolicy_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of csvserver_cspolicy_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/csvserver_cspolicy_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the csvserver_cspolicy_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "csvserver_cspolicy_binding": [ {

"targetlbvserver":<String_value>,

"policyname":<String_value>,

"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>,

"name":<String_value>,

"bindpoint":<String_value>,

"labeltype":<String_value>,

"priority":<Integer_value>,

"labelname":<String_value>,

"cookieipport":<String_value>,

"hits":<Integer_value>,

"pipolicyhits":<Integer_value>,

"vserverid":<String_value>,

"rule":<String_value>

}]}
```

get (all)

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver_cspolicy_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/csvserver_cspolicy_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "csvserver_cspolicy_binding": [ {

"targetlbvserver":<String_value>,

"policyname":<String_value>,

"gotopriorityexpression":<String_value>,

"invoke":<Boolean_value>,

"name":<String_value>,

"bindpoint":<String_value>,

"labeltype":<String_value>,
```

```
"priority":<Integer_value>,

"labelname":<String_value>,

"cookieipport":<String_value>,

"hits":<Integer_value>,

"pipolicyhits":<Integer_value>,

"vserverid":<String_value>,

"rule":<String_value>

}]}
```

count

URL: http:// <netscaler-ip-address> /nitro/v1/config/csvserver_cspolicy_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"csvserver_cspolicy_binding": [ { "__count": "#no"} ] }
```

lbvserver

Configuration for Load Balancing Virtual Server resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
name	<String>	Read-write	Name for the virtual server. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at sign (@), equal sign (=), and hyphen (-) characters. Can be changed after the virtual server is created. CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my vserver" or 'my vserver'). . Minimum length = 1
servicetype	<String>	Read-write	Protocol used by the service (also called the service type).

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = HTTP, FTP, TCP, UDP, SSL, SSL_BRIDGE, SSL_TCP, DTLS, NNTP, DNS, DHCPRA, ANY, SIP_UDP, SIP_TCP, SIP_SSL, DNS_TCP, RTSP, PUSH, SSL_PUSH, RADIUS, RDP, MYSQL, MSSQL, DIAMETER, SSL_DIAMETER, TFTP, ORACLE, SMPP, SYSLOGTCP, SYSLOGUDP, FIX, SSL_FIX, PROXY, USER_TCP, USER_SSL_TCP, QUIC, IPFIX, LOGSTREAM, MONGO, MONGO_TLS, MQTT, MQTT_TLS, QUIC_BRIDGE, HTTP_QUIC, DOT, SSL_PROXY, KAFKA_PRODUCER
ipv46	<String>	Read-write	IPv4 or IPv6 address to assign to the virtual server.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
ippattern	<String>	Read-write	IP address pattern, in dotted decimal notation, for identifying packets to be accepted by the virtual server. The IP Mask parameter specifies which part of the destination IP address is matched against the pattern. Mutually exclusive with the IP Address parameter. For example, if the IP pattern assigned to the virtual server is 198.51.100.0 and the IP mask is 255.255.240.0 (a forward mask), the first 20 bits in the destination IP addresses are matched with the first 20 bits in the pattern. The virtual server accepts requests with IP addresses that range from 198.51.96.1 to 198.51.111.254. You can also use a pattern such as 0.0.2.2 and a mask

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			such as 0.0.255.255 (a reverse mask). If a destination IP address matches more than one IP pattern, the pattern with the longest match is selected, and the associated virtual server processes the request. For example, if virtual servers vs1 and vs2 have the same IP pattern, 0.0.100.128, but different IP masks of 0.0.255.255 and 0.0.224.255, a destination IP address of 198.51.100.128 has the longest match with the IP pattern of vs1. If a destination IP address matches two or more virtual servers to the same extent, the request is processed by the virtual server whose port number matches the port

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			number in the request.
ipmask	<String>	Read-write	IP mask, in dotted decimal notation, for the IP Pattern parameter. Can have leading or trailing non-zero octets (for example, 255.255.240.0 or 0.0.255.255). Accordingly, the mask specifies whether the first n bits or the last n bits of the destination IP address in a client request are to be matched with the corresponding bits in the IP pattern. The former is called a forward mask. The latter is called a reverse mask.
port	<Integer>	Read-write	Port number for the virtual server. Range 1 - 65535 * in CLI is represented as 65535 in NITRO API
ipset	<String>	Read-write	The list of IPv4/IPv6 addresses bound to ipset would form a part of listening

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			service on the current lb vserver. Minimum length = 1
range	<Integer>	Read-write	Number of IP addresses that the appliance must generate and assign to the virtual server. The virtual server then functions as a network virtual server, accepting traffic on any of the generated IP addresses. The IP addresses are generated automatically, as follows: * For a range of n, the last octet of the address specified by the IP Address parameter increments n-1 times. * If the last octet exceeds 255, it rolls over to 0 and the third octet increments by 1. Note: The Range parameter assigns multiple IP addresses to one virtual server. To

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			generate an array of virtual servers, each of which owns only one IP address, use brackets in the IP Address and Name parameters to specify the range. For example: add lb vserver my_vserver[1-3] HTTP 192.0.2.[1-3] 80. Default value: 1 Minimum value = 1 Maximum value = 254
persistencetype	<String>	Read-write	Type of persistence for the virtual server. Available settings function as follows: * SOURCEIP - Connections from the same client IP address belong to the same persistence session. * COOKIEINSERT - Connections that have the same HTTP Cookie, inserted by a Set-

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Cookie directive from a server, belong to the same persistence session. * SSLSESSION - Connections that have the same SSL Session ID belong to the same persistence session. * CUSTOMSERVERID - Connections with the same server ID form part of the same session. For this persistence type, set the Server ID (CustomServerID) parameter for each service and configure the Rule parameter to identify the server ID in a request. * RULE - All connections that match a user defined rule belong to the same

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			persistence session. * URLPASSIVE - Requests that have the same server ID in the URL query belong to the same persistence session. The server ID is the hexadecimal representation of the IP address and port of the service to which the request must be forwarded. This persistence type requires a rule to identify the server ID in the request. * DESTIP - Connections to the same destination IP address belong to the same persistence session. * SRCIPDESTIP - Connections that have the same source IP address and destination IP address belong to the same

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			persistence session. * CALLID - Connections that have the same CALL-ID SIP header belong to the same persistence session. * RTSPSID - Connections that have the same RTSP Session ID belong to the same persistence session. * FIXSESSION - Connections that have the same SenderCompID and TargetCompID values belong to the same persistence session. * USERSESSION - Persistence session is created based on the persistence parameter value provided from an extension.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = SOURCEIP, COOKIEINSERT, SSLSESSION, RULE, URLPASSIVE, CUSTOMSERVERID, DESTIP, SRCIPDESTIP, CALLID, RTSPSID, DIAMETER, FIXSESSION, USERSESSION, NONE
timeout	<Integer>	Read-write	Time period for which a persistence session is in effect. Default value: 2 Minimum value = 0 Maximum value = 1440
persistencebackup	<String>	Read-write	Backup persistence type for the virtual server. Becomes operational if the primary persistence mechanism fails. Possible values = SOURCEIP, NONE
backuppersistencetimeout	<Integer>	Read-write	Time period for which backup persistence is in effect.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: 2 Minimum value = 2 Maximum value = 1440
lbmethod	<String>	Read-write	Load balancing method. The available settings function as follows: * ROUNDROBIN - Distribute requests in rotation, regardless of the load. Weights can be assigned to services to enforce weighted round robin distribution. * LEASTCONNECTION (default) - Select the service with the fewest connections. * LEASTRESPONSETIME - Select the service with the lowest average response time. * LEASTBANDWIDTH - Select the service currently

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			handling the least traffic. * LEASTPACKETS - Select the service currently serving the lowest number of packets per second. * CUSTOMLOAD - Base service selection on the SNMP metrics obtained by custom load monitors. * LRTM - Select the service with the lowest response time. Response times are learned through monitoring probes. This method also takes the number of active connections into account. Also available are a number of hashing methods, in which the appliance extracts a predetermined portion of the request, creates a hash of the portion,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			and then checks whether any previous requests had the same hash value. If it finds a match, it forwards the request to the service that served those previous requests. Following are the hashing methods: * URLHASH - Create a hash of the request URL (or part of the URL). * DOMAINHASH - Create a hash of the domain name in the request (or part of the domain name). The domain name is taken from either the URL or the Host header. If the domain name appears in both locations, the URL is preferred. If the request does not contain a domain name, the load balancing method defaults to

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			LEASTCONNECTION. * DESTINATIONIPHASH - Create a hash of the destination IP address in the IP header. * SOURCEIPHASH - Create a hash of the source IP address in the IP header. * TOKEN - Extract a token from the request, create a hash of the token, and then select the service to which any previous requests with the same token hash value were sent. * SRCIPDESTIPHASH - Create a hash of the string obtained by concatenating the source IP address and destination IP

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			address in the IP header. * SRCIPSRCPORTHASH - Create a hash of the source IP address and source port in the IP header. * CALLIDHASH - Create a hash of the SIP Call-ID header. * USER_TOKEN - Same as TOKEN LB method but token needs to be provided from an extension. * LEASTLLMTOKENLATENCY - Select the service with the least LLM token latency. Default value: LEASTCONNECTION Possible values = ROUNDROBIN, LEASTCONNECTION,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			LEASTRESPONSETIME, URLHASH, DOMAINHASH, DESTINATIONIPHASH, SOURCEIPHASH, SRCIPDESTIPHASH, LEASTBANDWIDTH, LEASTPACKETS, TOKEN, SRCIPSRCPORTHASH, LRTM, CALLIDHASH, CUSTOMLOAD, LEASTREQUEST, AUDITLOGHASH, STATICPROXIMITY, USER_TOKEN, LEASTLLMTOKEN LATENCY
hashlength	<Integer>	Read-write	Number of bytes to consider for the hash value used in the URLHASH and DOMAINHASH load balancing methods. Default value: 80 Minimum value = 1 Maximum value = 4096
netmask	<String>	Read-write	IPv4 subnet mask to apply to the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			destination IP address or source IP address when the load balancing method is DESTINATIONIPHASH or SOURCEIPHASH. Minimum length = 1
v6netmasklen	<Integer>	Read-write	Number of bits to consider in an IPv6 destination or source IP address, for creating the hash that is required by the DESTINATIONIPHASH and SOURCEIPHASH load balancing methods. Default value: 128 Minimum value = 1 Maximum value = 128
backuplbmethod	<String>	Read-write	Backup load balancing method. Becomes operational if the primary load balancing me thod fails or cannot be used. Valid only if the primary method is

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			based on static proximity. Default value: ROUNDROBIN Possible values = ROUNDROBIN, LEASTCONNECTION, LEASTRESPONSETIME, SOURCEIPHASH, LEASTBANDWIDTH, LEASTPACKETS, CUSTOMLOAD
aigwprofilename	<String>	Read-write	Name of the AIGW frontend profile. For the LB vserver to function as AI gateway, this parameter must be set. Once this parameter is set using add lb vserver, it cannot be unset. Minimum length = 1 Maximum length = 255
cookiename	<String>	Read-write	Use this parameter to specify the cookie name for COOKIE peristence type. It specifies the name of cookie with a maximum of 32

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			characters. If not specified, cookie name is internally generated.
rule	<String>	Read-write	Expression, or name of a named expression, against which traffic is evaluated. The following requirements apply only to the Citrix ADC CLI: * If the expression includes one or more spaces, enclose the entire expression in double quotation marks. * If the expression itself includes double quotation marks, escape the quotations by using the \ character. * Alternatively, you can use single quotation marks to enclose the rule, in which case you do not have to escape

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			the double quotation marks. Default value: "none"
listenpolicy	<String>	Read-write	Expression identifying traffic accepted by the virtual server. Can be either an expression (for example, CLIENT.IP.DST.IN_SUBNET(192.0.2.0/24) or the name of a named expression. In the above example, the virtual server accepts all requests whose destination IP address is in the 192.0.2.0/24 subnet. Default value: "NONE"
listenpriority	<Integer>	Read-write	Integer specifying the priority of the listen policy. A higher number specifies a lower priority. If a request matches the listen policies of more than one virtual server the virtual server whose listen policy has the highest priority (the lowest priority

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			number) accepts the request. Default value: 101 Minimum value = 0 Maximum value = 101
resrule	<String>	Read-write	Expression specifying which part of a server's response to use for creating rule based persistence sessions (persistence type RULE). Can be either an expression or the name of a named expression. Example: HTTP.RES.HEADER("setcookie").VALUE(0).TYPECAST_NVLIST_T('=',';').VALUE("server1"). Default value: "none"
persistmask	<String>	Read-write	Persistence mask for IP based persistence types, for IPv4 virtual servers. Minimum length = 1
v6persistmasklen	<Integer>	Read-write	Persistence mask for IP based persistence

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			types, for IPv6 virtual servers. Default value: 128 Minimum value = 1 Maximum value = 128
rtspnat	<String>	Read-write	Use network address translation (NAT) for RTSP data connections. Default value: OFF Possible values = ON, OFF
m	<String>	Read-write	Redirection mode for load balancing. Available settings function as follows: * IP - Before forwarding a request to a server, change the destination IP address to the server's IP address. * MAC - Before forwarding a request to a server, change the destination MAC address to the server's MAC address. The destination IP

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			address is not changed. MAC-based redirection mode is used mostly in firewall load balancing deployments. * IPTUNNEL - Perform IP-in-IP encapsulation for client IP packets. In the outer IP headers, set the destination IP address to the IP address of the server and the source IP address to the subnet IP (SNIP). The client IP packets are not modified. Applicable to both IPv4 and IPv6 packets. * TOS - Encode the virtual server's TOS ID in the TOS field of the IP header. You can use either the IPTUNNEL or the TOS option to implement Direct

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Server Return (DSR). Default value: IP Possible values = IP, MAC, IPTUNNEL, TOS
tosid	<Integer>	Read-write	TOS ID of the virtual server. Applicable only when the load balancing redirection mode is set to TOS. Minimum value = 1 Maximum value = 63
datalength	<Integer>	Read-write	Length of the token to be extracted from the data segment of an incoming packet, for use in the token method of load balancing. The length of the token, specified in bytes, must not be greater than 24 KB. Applicable to virtual servers of type TCP. Minimum value = 1 Maximum value = 100
dataoffset	<Integer>	Read-write	Offset to be considered when extracting a token from the TCP

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			payload. Applicable to virtual servers, of type TCP, using the token method of load balancing. Must be within the first 24 KB of the TCP payload. Minimum value = 0 Maximum value = 25400
sessionless	<String>	Read-write	Perform load balancing on a per-packet basis, without establishing sessions. Recommended for load balancing of intrusion detection system (IDS) servers and scenarios involving direct server return (DSR), where session information is unnecessary. Default value: DISABLED Possible values = ENABLED, DISABLED
trofspersistence	<String>	Read-write	When value is ENABLED, Trofs persistence is honored. When value is DISABLED,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Trofs persistence is not honored. Default value: ENABLED Possible values = ENABLED, DISABLED
state	<String>	Read-write	State of the load balancing virtual server. Default value: ENABLED Possible values = ENABLED, DISABLED
connfailover	<String>	Read-write	Mode in which the connection failover feature must operate for the virtual server. After a failover, established TCP connections and UDP packet flows are kept active and resumed on the secondary appliance. Clients remain connected to the same servers. Available settings function as follows: * STATEFUL - The primary appliance shares state information with the secondary

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			appliance, in real time, resulting in some runtime processing overhead. * STATELESS - State information is not shared, and the new primary appliance tries to re-create the packet flow on the basis of the information contained in the packets it receives. * DISABLED - Connection failover does not occur. Default value: DISABLED Possible values = DISABLED, STATEFUL, STATELESS
redirurl	<String>	Read-write	URL to which to redirect traffic if the virtual server becomes unavailable. WARNING! Make sure that the domain in the URL does not match the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			domain specified for a content switching policy. If it does, requests are continuously redirected to the unavailable virtual server. Minimum length = 1
cacheable	<String>	Read-write	Route cacheable requests to a cache redirection virtual server. The load balancing virtual server can forward requests only to a transparent cache redirection virtual server that has an IP address and port combination of *:80, so such a cache redirection virtual server must be configured on the appliance. Default value: NO Possible values = YES, NO
clttimeout	<Integer>	Read-write	Idle time, in seconds, after which a client connection is terminated. Minimum value = 0

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum value = 31536000
somethod	<String>	Read-write	Type of threshold that, when exceeded, triggers spillover. Available settings function as follows: * CONNECTION - Spillover occurs when the number of client connections exceeds the threshold. * DYNAMICCONNECTION - Spillover occurs when the number of client connections at the virtual server exceeds the sum of the maximum client (Max Clients) settings for bound services. Do not specify a spillover threshold for this setting, because the threshold is implied by the Max Clients settings of bound services.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			* BANDWIDTH - Spillover occurs when the bandwidth consumed by the virtual server's incoming and outgoing traffic exceeds the threshold. * HEALTH - Spillover occurs when the percentage of weights of the services that are UP drops below the threshold. For example, if services svc1, svc2, and svc3 are bound to a virtual server, with weights 1, 2, and 3, and the spillover threshold is 50%, spillover occurs if svc1 and svc3 or svc2 and svc3 transition to DOWN. * LLMQUOTA - Spillover occurs when the LLM token quota of all the services bound the vserver is exhausted. Do not

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			specify a spillover threshold for this setting, because the threshold is implied by the max tokens settings on the bound services. * NONE - Spillover does not occur. Possible values = CONNECTION, DYNAMICCONNECTION, BANDWIDTH, HEALTH, LLMQUOTA, NONE
sopersistence	<String>	Read-write	If spillover occurs, maintain source IP address based persistence for both primary and backup virtual servers. Default value: DISABLED Possible values = ENABLED, DISABLED
sopersistencetimeout	<Integer>	Read-write	Timeout for spillover persistence, in minutes. Default value: 2 Minimum value = 2

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Maximum value = 1440
healththreshold	<Integer>	Read-write	Threshold in percent of active services below which vserver state is made down. If this threshold is 0, vserver state will be up even if one bound service is up. Default value: 0 Minimum value = 0 Maximum value = 100
sothreshold	<Integer>	Read-write	Threshold at which spillover occurs. Specify an integer for the CONNECTION spillover method, a bandwidth value in kilobits per second for the BANDWIDTH method (do not enter the units), or a percentage for the HEALTH method (do not enter the percentage symbol). Minimum value = 1 Maximum value = 4294967287
sobackupaction	<String>	Read-write	Action to be performed if spillover is to take effect, but no backup chain to

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			spillover is usable or exists. Possible values = DROP, ACCEPT, REDIRECT
redirectportrewrite	<String>	Read-write	Rewrite the port and change the protocol to ensure successful HTTP redirects from services. Default value: DISABLED Possible values = ENABLED, DISABLED
downstateflush	<String>	Read-write	Flush all active transactions associated with a virtual server whose state transitions from UP to DOWN. Do not enable this option for applications that must complete their transactions. Default value: ENABLED Possible values = ENABLED, DISABLED
backupvserver	<String>	Read-write	Name of the backup virtual server to which to forward requests if the primary virtual server

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			goes DOWN or reaches its spillover threshold. Minimum length = 1
disableprimaryondown	<String>	Read-write	If the primary virtual server goes down, do not allow it to return to primary status until manually enabled. Default value: DISABLED Possible values = ENABLED, DISABLED
insertvserveripport	<String>	Read-write	Insert an HTTP header, whose value is the IP address and port number of the virtual server, before forwarding a request to the server. The format of the header is <vipHeader>: <virtual server IP address>_<port number >, where vipHeader is the name that you specify for the header. If the virtual server has an IPv6 address, the address in the header is enclosed in brackets ([and]) to separate it from the port number. If you have

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			mapped an IPv4 address to a virtual server's IPv6 address, the value of this parameter determines which IP address is inserted in the header, as follows: * VIPADDR - Insert the IP address of the virtual server in the HTTP header regardless of whether the virtual server has an IPv4 address or an IPv6 address. A mapped IPv4 address, if configured, is ignored. * V6TOV4MAPPING - Insert the IPv4 address that is mapped to the virtual server's IPv6 address. If a mapped IPv4 address is not configured, insert the IPv6 address. * OFF - Disable header insertion.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = OFF, VIPADDR, V6TOV4MAPPING
vipheader	<String>	Read-write	Name for the inserted header. The default name is vip-header. Minimum length = 1
authenticationhost	<String>	Read-write	Fully qualified domain name (FQDN) of the authentication virtual server to which the user must be redirected for authentication. Make sure that the Authentication parameter is set to ENABLED. Minimum length = 3 Maximum length = 252
authentication	<String>	Read-write	Enable or disable user authentication. Default value: OFF Possible values = ON, OFF
authn401	<String>	Read-write	Enable or disable user authentication with HTTP 401 responses. Default value: OFF

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ON, OFF
authnvsname	<String>	Read-write	Name of an authentication virtual server with which to authenticate users. Minimum length = 1 Maximum length = 252
push	<String>	Read-write	Process traffic with the push virtual server that is bound to this load balancing virtual server. Default value: DISABLED Possible values = ENABLED, DISABLED
pushvserver	<String>	Read-write	Name of the load balancing virtual server, of type PUSH or SSL_PUSH, to which the server pushes updates received on the load balancing virtual server that you are configuring. Minimum length = 1
pushlabel	<String>	Read-write	Expression for extracting a label from the server's response. Can be either an expression

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			or the name of a named expression. Default value: "none"
pushmulticlients	<String>	Read-write	Allow multiple Web 2.0 connections from the same client to connect to the virtual server and expect updates. Default value: NO Possible values = YES, NO
tcpprofilename	<String>	Read-write	Name of the TCP profile whose settings are to be applied to the virtual server. Minimum length = 1 Maximum length = 127
httpprofilename	<String>	Read-write	Name of the HTTP profile whose settings are to be applied to the virtual server. Minimum length = 1 Maximum length = 127
dbprofilename	<String>	Read-write	Name of the DB profile whose settings are to be

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			applied to the virtual server. Minimum length = 1 Maximum length = 127
mcpprofilename	<String>	Read-write	Name of the MCP profile to attach to this lb vserver. Enables MCP protocol processing.
comment	<String>	Read-write	Any comments that you might want to associate with the virtual server.
l2conn	<String>	Read-write	Use Layer 2 parameters (channel number, MAC address, and VLAN ID) in addition to the 4-tuple (<source IP>:<source port>::<destination IP>:<destination port>) that is used to identify a connection. Allows multiple TCP and non-TCP connections with the same 4-tuple to co-exist on the Citrix ADC. Possible values = ON, OFF
oracleserverversion	<String>	Read-write	Oracle server version.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Default value: 10G Possible values = 10G, 11G
mssqlserverversion	<String>	Read-write	For a load balancing virtual server of type MSSQL, the Microsoft SQL Server version. Set this parameter if you expect some clients to run a version different from the version of the database. This setting provides compatibility between the client-side and server-side connections by ensuring that all communication conforms to the server's version. Default value: 2008R2 Possible values = 70, 2000, 2000SP1, 2005, 2008, 2008R2, 2012, 2014
mysqlprotocolversion	<Integer>	Read-write	MySQL protocol version that the virtual server advertises to clients.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
mysqlserverversion	<String>	Read-write	MySQL server version string that the virtual server advertises to clients. Minimum length = 1 Maximum length = 31
mysqlcharacterset	<Integer>	Read-write	Character set that the virtual server advertises to clients.
mysqlservercapabilities	<Integer>	Read-write	Server capabilities that the virtual server advertises to clients.
appflowlog	<String>	Read-write	Apply AppFlow logging to the virtual server. Default value: ENABLED Possible values = ENABLED, DISABLED
netprofile	<String>	Read-write	Name of the network profile to associate with the virtual server. If you set this parameter, the virtual server uses only the IP addresses in the network profile as source IP addresses when initiating connections with servers.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum length = 1 Maximum length = 127
icmpvsrresponse	<String>	Read-write	How the Citrix ADC responds to ping requests received for an IP address that is common to one or more virtual servers. Available settings function as follows: * If set to PASSIVE on all the virtual servers that share the IP address, the appliance always responds to the ping requests. * If set to ACTIVE on all the virtual servers that share the IP address, the appliance responds to the ping requests if at least one of the virtual servers is UP. Otherwise, the appliance does not respond. * If set to ACTIVE on some virtual servers and PASSIVE on the others, the

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			appliance responds if at least one virtual server with the ACTIVE setting is UP. Otherwise, the appliance does not respond. Note: This parameter is available at the virtual server level. A similar parameter, ICMP Response, is available at the IP address level, for IPv4 addresses of type VIP. To set that parameter, use the add ip command in the CLI or the Create IP dialog box in the GUI. Default value: PASSIVE Possible values = PASSIVE, ACTIVE
rhistate	<String>	Read-write	Route Health Injection (RHI) functionality of the NetSaler appliance for advertising the route of the VIP address associated with the virtual

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			server. When Vserver RHI Level (RHI) parameter is set to VSVR_CNTRLD, the following are different RHI behaviors for the VIP address on the basis of RHIstate (RHI STATE) settings on the virtual servers associated with the VIP address: * If you set RHI STATE to PASSIVE on all virtual servers, the Citrix ADC always advertises the route for the VIP address. * If you set RHI STATE to ACTIVE on all virtual servers, the Citrix ADC advertises the route for the VIP address if at least one of the associated virtual servers is in UP state. * If you set RHI STATE to ACTIVE on some and PASSIVE on others,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			the Citrix ADC advertises the route for the VIP address if at least one of the associated virtual servers, whose RHI STATE set to ACTIVE, is in UP state. Default value: PASSIVE Possible values = PASSIVE, ACTIVE
newservicerequest	<Integer>	Read-write	Number of requests, or percentage of the load on existing services, by which to increase the load on a new service at each interval in slow-start mode. A non-zero value indicates that slow-start is applicable. A zero value indicates that the global RR startup parameter is applied. Changing the value to zero will cause services currently in slow start to take the full traffic as determined by the LB method. Subsequently, any new services added

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			will use the global RR factor. Default value: 0
newservicerequestunit	<String>	Read-write	Units in which to increment load at each interval in slow-start mode. Default value: PER_SECOND Possible values = PER_SECOND, PERCENT
newservicerequestincrementinterval	<Integer>	Read-write	Interval, in seconds, between successive increments in the load on a new service or a service whose state has just changed from DOWN to UP. A value of 0 (zero) specifies manual slow start. Default value: 0 Minimum value = 0 Maximum value = 3600
minautoscalemembers	<Integer>	Read-write	Minimum number of members expected to be present when vserver is used in Autoscale. Default value: 0

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum value = 0 Maximum value = 5000
maxautoscalemembers	<Integer>	Read-write	Maximum number of members expected to be present when vserver is used in Autoscale. Default value: 0 Minimum value = 0 Maximum value = 5000
persistavpno	<Integer[]>	Read-write	Persist AVP number for Diameter Persistency. In case this AVP is not defined in Base RFC 3588 and it is nested inside a Grouped AVP, define a sequence of AVP numbers (max 3) in order of parent to child. So say persist AVP number X is nested inside AVP Y which is nested in Z, then define the list as Z Y X. Minimum value = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
skippersistency	<String>	Read-write	This argument decides the behavior incase the service which is selected from an existing persistence session has reached threshold. Default value: None Possible values = Bypass, ReLb, None
td	<Integer>	Read-write	Integer value that uniquely identifies the traffic domain in which you want to configure the entity. If you do not specify an ID, the entity becomes part of the default traffic domain, which has an ID of 0. Minimum value = 0 Maximum value = 4094
authnprofile	<String>	Read-write	Name of the authentication profile to be used when authentication is turned on.
macmoderetainvlan	<String>	Read-write	This option is used to retain vlan information of incoming packet

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			when macmode is enabled. Default value: DISABLED Possible values = ENABLED, DISABLED
dbslb	<String>	Read-write	Enable database specific load balancing for MySQL and MSSQL service types. Default value: DISABLED Possible values = ENABLED, DISABLED
dns64	<String>	Read-write	This argument is for enabling/disabling the dns64 on lbvserver. Possible values = ENABLED, DISABLED
bypassaaaa	<String>	Read-write	If this option is enabled while resolving DNS64 query AAAA queries are not sent to back end dns server. Default value: NO Possible values = YES, NO

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
recursionavailable	<String>	Read-write	When set to YES, this option causes the DNS replies from this vserver to have the RA bit turned on. Typically one would set this option to YES, when the vserver is load balancing a set of DNS servers thatsupport recursive queries. Default value: NO Possible values = YES, NO
processlocal	<String>	Read-write	By turning on this option packets destined to a vserver in a cluster will not under go any steering. Turn this option for single packet request response mode or when the upstream device is performing a proper RSS for connection based distribution. Default value: DISABLED Possible values = ENABLED, DISABLED

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
dnsprofilename	<String>	Read-write	Name of the DNS profile to be associated with the VServer. DNS profile properties will be applied to the transactions processed by a VServer. This parameter is valid only for DNS and DNS-TCP VServers. Minimum length = 1 Maximum length = 127
lbprofilename	<String>	Read-write	Name of the LB profile which is associated to the vserver.
redirectfromport	<Integer>	Read-write	Port number for the virtual server, from which we absorb the traffic for http redirect. Minimum value = 1 Range 1 - 65535 * in CLI is represented as 65535 in NITRO API
httpsredirecturl	<String>	Read-write	URL to which all HTTP traffic received on the port specified in the -redirectFromPort

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			parameter is redirected.
retainconnectionsoncluster	<String>	Read-write	This option enables you to retain existing connections on a node joining a Cluster system or when a node is being configured for passive timeout. By default, this option is disabled. Default value: NO Possible values = YES, NO
adfsproxyprofile	<String>	Read-write	Name of the adfsProxy profile to be used to support ADFSPIP protocol for ADFS servers.
tcpprobeport	<Integer>	Read-write	Port number for external TCP probe. NetScaler provides support for external TCP health check of the vserver status over the selected port. This option is only supported for vservers assigned with an IPAddress or ipset. Minimum value = 1 Range 1 - 65535

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			* in CLI is represented as 65535 in NITRO API
quicprofilename	<String>	Read-write	Name of QUIC profile which will be attached to the VServer. Minimum length = 1 Maximum length = 255
quicbridgeprofilename	<String>	Read-write	Name of the QUIC Bridge profile whose settings are to be applied to the virtual server. Minimum length = 1 Maximum length = 127
probeprotocol	<String>	Read-write	Citrix ADC provides support for external health check of the vserver status. Select HTTP or TCP probes for healthcheck. Possible values = TCP, HTTP
probesuccessresponsecode	<String>	Read-write	HTTP code to return in SUCCESS case. Default value: "200 OK"

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum length = 1 Maximum length = 64
probeport	<Integer>	Read-write	Citrix ADC provides support for external health check of the vserver status. Select port for HTTP/ TCP monitring. Default value: 0 Range 1 - 65535 * in CLI is represented as 65535 in NITRO API
toggleorder	<String>	Read-write	Configure this option to toggle order preference. Default value: ASCENDING Possible values = ASCENDING, DESCENDING
orderthreshold	<Integer>	Read-write	This option is used to to specify the threshold of minimum number of services to be UP in an order, for it to be considered in Lb decision. Default value: 0

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Minimum value = 0 Maximum value = 100
apiprofile	<String>	Read-write	The API profile where one or more API specs are bounded to. Minimum length = 1
dnsoverhttps	<String>	Read-write	This option is used to enable/disable DNS over HTTPS (DoH) processing. Default value: DISABLED Possible values = ENABLED, DISABLED
wasmmodule	<String>	Read-write	Name of the WASM module to assign to this virtual server.
servicename	<String>	Read-write	Service to bind to the virtual server. Minimum length = 1
weight	<Integer>	Read-write	Weight to assign to the specified service. Minimum value = 1 Maximum value = 100
order	<Integer>	Read-write	Order number to be assigned to the service when it is

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			bound to the lb vserver. Minimum value = 1 Maximum value = 8192
redirurlflags	<Boolean>	Read-write	The redirect URL to be unset.
newname	<String>	Read-write	New name for the virtual server. Minimum length = 1
value	<String>	Read-only	SSL status. Possible values = Certkey/ Certkeybundle/Vault not bound/Cert-store not usable, SSL feature disabled
ipmapping	<String>	Read-only	The permanent mapping for the V6 Address.
ngname	<String>	Read-only	Nodegroup name to which this lbvsever belongs to.
type	<String>	Read-only	Type of LB vserver. Possible values = CONTENT, ADDRESS
curstate	<String>	Read-only	Current LB vserver state.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = UP, DOWN, UNKNOWN, BUSY, OUT OF SERVICE, GOING OUT OF SERVICE, DOWN WHEN GOING OUT OF SERVICE, NS_EMPTY_STR, Unknown, DISABLED
effectivestate	<String>	Read-only	Effective state of the LB vserver , based on the state of backup vservers. Possible values = UP, DOWN, UNKNOWN, BUSY, OUT OF SERVICE, GOING OUT OF SERVICE, DOWN WHEN GOING OUT OF SERVICE, NS_EMPTY_STR, Unknown, DISABLED
status	<Integer>	Read-only	Current status of the lb vserver. During the initial phase if the configured lb method is not round robin , the vserver will adopt round robin to distribute traffic for a predefined number of requests.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
lbrrreason	<Integer>	Read-only	Reason why a vserver is in RR. The following are the reasons: 1 - MEP is DOWN (GSLB) 2 - LB method has changed 3 - Bound service's state changed to UP 4 - A new service is bound 5 - Startup RR factor has changed 6 - LB feature is enabled 7 - Load monitor is not active on a service 8 - Vserver is Enabled 9 - SSL feature is Enabled 10 - All bound services have reached threshold. Using effective state to load balance (GSLB)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			11 - Primary state of bound services are not UP. Using effective state to load balance (GSLB) 12 - No LB decision can be made as all bound services have either reached threshold or are not UP (GSLB) 13 - All load monitors are active .
redirect	<String>	Read-only	Cache redirect type. Possible values = CACHE, POLICY, ORIGIN
precedence	<String>	Read-only	Precedence. Possible values = RULE, URL
homepage	<String>	Read-only	Home page.
dnsvservername	<String>	Read-only	DNS vserver name.
domain	<String>	Read-only	Domain.
cachevserver	<String>	Read-only	Cache virtual server.
health	<Integer>	Read-only	Health of vserver based on percentage of weights of active svcs/all svcs. This

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			does not consider administratively disabled svcs.
ruletype	<Integer>	Read-only	Rule type.
groupname	<String>	Read-only	LB group to which the lb vserver is to be bound.
cookiedomain	<String>	Read-only	Domain name to be used in the set cookie header in case of cookie persistence.
map	<String>	Read-only	Map. Possible values = ON, OFF
gt2gb	<String>	Read-only	Allow for greater than 2 GB transactions on this vserver. Default value: DISABLED Possible values = ENABLED, DISABLED
consolidatedlconn	<String>	Read-only	Use consolidated stats for LeastConnection. Default value: GLOBAL Possible values = GLOBAL, NO, YES

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
consolidatedlconngbl	<String>	Read-only	Fetches Global setting. Possible values = YES, NO
thresholdvalue	<Integer>	Read-only	Tells whether threshold exceeded for this service participating in CUSTOMLB.
bindpoint	<String>	Read-only	The bindpoint to which the policy is bound. Possible values = REQUEST, RESPONSE, MQTT_JUMBO_REQ
version	<Integer>	Read-only	Cookie version.
totalservices	<Integer>	Read-only	Total number of services bound to the vserver.
activeservices	<Integer>	Read-only	Total number of active services bound to the vserver.
statechangetimesec	<String>	Read-only	Time when last state change happened. Seconds part.
statechangetimeseconds	<Integer>	Read-only	Time when last state change happened. Seconds part.
statechangetimemsec	<Integer>	Read-only	Time at which last state change

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			happened. Milliseconds part.
tickssincelaststatechange	<Integer>	Read-only	Time in 10 millisecond ticks since the last state change.
isgslb	<Boolean>	Read-only	This field is set to true if it is a GSLBVserver.
vsvrdynconnsothreshold	<Integer>	Read-only	Spillover threshold for dynamic connection.
backupvserverstatus	<String>	Read-only	Staus of BackUp Vserver .
nodefaultbindings	<String>	Read-only	to determine if the configuration will have default ssl CIPHER and ECC curve bindings. Default value: NO Possible values = YES, NO
currentactiveorder	<String>	Read-only	current order that takes the traffic in case service or servicegroup is bound with order.
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- ENABLE
- DISABLE
- GET (ALL)
- GET
- COUNT
- RENAME

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

add

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"lbvserver":{

<b>"name":<String_value>,

</b><b>"servicetype":<String_value>,

</b>"ipv46":<String_value>,

"ippattern":<String_value>,

"ipmask":<String_value>,

"port":<Integer_value>,

"ipset":<String_value>,

"range":<Integer_value>,

"persistencetype":<String_value>,

"timeout":<Integer_value>,

"persistencebackup":<String_value>,

"backuppersistencetimeout":<Integer_value>,

"lbmethod":<String_value>,

"hashlength":<Integer_value>,

"netmask":<String_value>,
```

```
"v6netmasklen":<Integer_value>,

"backuplbmethod":<String_value>,

"aigwprofilename":<String_value>,

"cookiename":<String_value>,

"rule":<String_value>,

"listenpolicy":<String_value>,

"listenpriority":<Integer_value>,

"resrule":<String_value>,

"persistmask":<String_value>,

"v6persistmasklen":<Integer_value>,

"rtspnat":<String_value>,

"m":<String_value>,

"tosid":<Integer_value>,

"datalength":<Integer_value>,

"dataoffset":<Integer_value>,

"sessionless":<String_value>,

"trofspersistence":<String_value>,

"state":<String_value>,

"connfailover":<String_value>,

"redirurl":<String_value>,

"cacheable":<String_value>,

"clttimeout":<Integer_value>,
```

```
"somethod":<String_value>,

"sopersistence":<String_value>,

"sopersistencetimeout":<Integer_value>,

"healththreshold":<Integer_value>,

"sothreshold":<Integer_value>,

"sobackupaction":<String_value>,

"redirectportrewrite":<String_value>,

"downstateflush":<String_value>,

"backupvserver":<String_value>,

"disableprimaryondown":<String_value>,

"insertvserveripport":<String_value>,

"vipheader":<String_value>,

"authenticationhost":<String_value>,

"authentication":<String_value>,

"authn401":<String_value>,

"authnvsname":<String_value>,

"push":<String_value>,

"pushvserver":<String_value>,

"pushlabel":<String_value>,

"pushmulticlients":<String_value>,

"tcpprofilename":<String_value>,

"httpprofilename":<String_value>,
```

```
"dbprofilename":<String_value>,

"mcpprofilename":<String_value>,

"comment":<String_value>,

"l2conn":<String_value>,

"oracleserverversion":<String_value>,

"mssqlserverversion":<String_value>,

"mysqlprotocolversion":<Integer_value>,

"mysqlserverversion":<String_value>,

"mysqlcharacterset":<Integer_value>,

"mysqlservercapabilities":<Integer_value>,

"appflowlog":<String_value>,

"netprofile":<String_value>,

"icmpvsrresponse":<String_value>,

"rhistate":<String_value>,

"newservicerequest":<Integer_value>,

"newservicerequestunit":<String_value>,

"newservicerequestincrementinterval":<Integer_value>,

"minautoscalemembers":<Integer_value>,

"maxautoscalemembers":<Integer_value>,

"persistavpno":<Integer[]_value>,

"skippersistency":<String_value>,

"td":<Integer_value>,
```

```
"authnprofile":<String_value>,

"macmoderetainvlan":<String_value>,

"dbslb":<String_value>,

"dns64":<String_value>,

"bypassaaaa":<String_value>,

"recursionavailable":<String_value>,

"processlocal":<String_value>,

"dnsprofilename":<String_value>,

"lbprofilename":<String_value>,

"redirectfromport":<Integer_value>,

"httpsredirecturl":<String_value>,

"retainconnectionsoncluster":<String_value>,

"adfsproxyprofile":<String_value>,

"tcpprobeport":<Integer_value>,

"quicprofilename":<String_value>,

"quicbridgeprofilename":<String_value>,

"probeprotocol":<String_value>,

"probesuccessresponsecode":<String_value>,

"probeport":<Integer_value>,

"togglеorder":<String_value>,

"orderthreshold":<Integer_value>,

"apiprofile":<String_value>,
```

```
"dnsoverhttps":<String_value>,

"wasmmodule":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

delete

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver/ name_value<String> **HTTP Method:** DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

update

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"lbvserver":{

<b>"name":<String_value>,

</b>"ipv46":<String_value>,
```

```
"ipset":<String_value>,

"ippattern":<String_value>,

"ipmask":<String_value>,

"servicename":<String_value>,

"weight":<Integer_value>,

"order":<Integer_value>,

"persistencetype":<String_value>,

"timeout":<Integer_value>,

"persistencebackup":<String_value>,

"backuppersistencetimeout":<Integer_value>,

"lbmethod":<String_value>,

"hashlength":<Integer_value>,

"netmask":<String_value>,

"v6netmasklen":<Integer_value>,

"backuplbmethod":<String_value>,

"rule":<String_value>,

"cookiename":<String_value>,

"resrule":<String_value>,

"persistmask":<String_value>,

"v6persistmasklen":<Integer_value>,

"rtspnat":<String_value>,

"m":<String_value>,
```

```
"tosid":<Integer_value>,

"datalength":<Integer_value>,

"dataoffset":<Integer_value>,

"sessionless":<String_value>,

"trofspersistence":<String_value>,

"connfailover":<String_value>,

"backupvserver":<String_value>,

"redirurl":<String_value>,

"cacheable":<String_value>,

"clttimeout":<Integer_value>,

"somethod":<String_value>,

"sothreshold":<Integer_value>,

"sopersistence":<String_value>,

"sopersistencetimeout":<Integer_value>,

"healththreshold":<Integer_value>,

"sobackupaction":<String_value>,

"redirectportrewrite":<String_value>,

"downstateflush":<String_value>,

"insertvserveripport":<String_value>,

"vipheader":<String_value>,

"disableprimaryondown":<String_value>,

"authenticationhost":<String_value>,
```

```
"authentication":<String_value>,

"authn401":<String_value>,

"authnvsname":<String_value>,

"push":<String_value>,

"pushvserver":<String_value>,

"pushlabel":<String_value>,

"pushmulticlients":<String_value>,

"listenpolicy":<String_value>,

"listenpriority":<Integer_value>,

"tcpprofilename":<String_value>,

"httpprofilename":<String_value>,

"dbprofilename":<String_value>,

"mcpprofilename":<String_value>,

"comment":<String_value>,

"l2conn":<String_value>,

"oracleserverversion":<String_value>,

"mssqlserverversion":<String_value>,

"mysqlprotocolversion":<Integer_value>,

"mysqlserverversion":<String_value>,

"mysqlcharacterset":<Integer_value>,

"mysqlservercapabilities":<Integer_value>,

"appflowlog":<String_value>,
```

```
"netprofile":<String_value>,

"icmpvsrresponse":<String_value>,

"rhistate":<String_value>,

"newservicerequest":<Integer_value>,

"newservicerequestunit":<String_value>,

"newservicerequestincrementinterval":<Integer_value>,

"minautoscalemembers":<Integer_value>,

"maxautoscalemembers":<Integer_value>,

"persistavpno":<Integer[]_value>,

"skippersistency":<String_value>,

"authnprofile":<String_value>,

"macmoderetainvlan":<String_value>,

"dbslb":<String_value>,

"dns64":<String_value>,

"bypassaaaa":<String_value>,

"recursionavailable":<String_value>,

"processlocal":<String_value>,

"dnsprofilename":<String_value>,

"lbprofilename":<String_value>,

"redirectfromport":<Integer_value>,

"httpsredirecturl":<String_value>,

"retainconnectionsoncluster":<String_value>,
```

```
"adfsproxyprofile":<String_value>,

"tcpprobeport":<Integer_value>,

"quicprofilename":<String_value>,

"quicbridgeprofilename":<String_value>,

"probeport":<Integer_value>,

"probeprotocol":<String_value>,

"probesuccessresponsecode":<String_value>,

"togglеorder":<String_value>,

"orderthreshold":<Integer_value>,

"apiprofile":<String_value>,

"dnsoverhttps":<String_value>,

"wasmmodule":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

unset

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"lbvserver":{

<b>"name":<String_value>,

</b>"backupvserver":true,

"clttimeout":true,

"redirurl":true,

"redirurlflags":true,

"authn401":true,

"authentication":true,

"authenticationhost":true,

"authnvsname":true,

"pushvserver":true,

"pushlabel":true,

"tcpprofilename":true,

"httpprofilename":true,

"dbprofilename":true,

"rule":true,

"sothreshold":true,

"l2conn":true,

"mysqlprotocolversion":true,

"mysqlserverversion":true,

"mysqlcharacterset":true,
```

```
"mysqlservercapabilities":true,

"appflowlog":true,

"netprofile":true,

"icmpvsrresponse":true,

"skippersistency":true,

"minautoscalemembers":true,

"maxautoscalemembers":true,

"authnprofile":true,

"macmoderetainvlan":true,

"dbslb":true,

"dnsprofilename":true,

"lbprofilename":true,

"redirectfromport":true,

"httpsredirecturl":true,

"adfsproxyprofile":true,

"tcpprobeport":true,

"quicprofilename":true,

"quicbridgeprofilename":true,

"probeprotocol":true,

"servicename":true,

"order":true,

"apiprofile":true,
```

```
"dnsoverhttps":true,

"wasmmodule":true,

"ipset":true,

"persistencetype":true,

"timeout":true,

"persistencebackup":true,

"backuppersistencetimeout":true,

"lbmethod":true,

"hashlength":true,

"netmask":true,

"v6netmasklen":true,

"backuplbmethod":true,

"cookiename":true,

"resrule":true,

"persistmask":true,

"v6persistmasklen":true,

"rtspnat":true,

"m":true,

"tosid":true,

"datalength":true,

"dataoffset":true,

"sessionless":true,
```

```
"trofspersistence":true,

"connfailover":true,

"cacheable":true,

"somethod":true,

"sopersistence":true,

"sopersistencetimeout":true,

"healththreshold":true,

"sobackupaction":true,

"redirectportrewrite":true,

"downstateflush":true,

"insertvserveripport":true,

"vipheader":true,

"disableprimaryondown":true,

"push":true,

"pushmulticlients":true,

"listenpolicy":true,

"listenpriority":true,

"mcpprofilename":true,

"comment":true,

"oracleserverversion":true,

"mssqlserverversion":true,

"rhistate":true,
```

```
"newservicerequest":true,

"newservicerequestunit":true,

"newservicerequestincrementinterval":true,

"persistavpno":true,

"recursionavailable":true,

"retainconnectionsoncluster":true,

"probesuccessresponsecode":true,

"toggleorder":true,

"orderthreshold":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

enable

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver? **action=enable HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"lbvserver":{

<b>"name":<String_value>
```

```
</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

disable

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver? **action=disable HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"lbvserver":{

<b>"name":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

rename

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver? **action=rename HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"lbvserver":{

<b>"name":<String_value>,

</b><b>"newname":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

get (all)

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/lbvserver? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/lbvserver? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of lbvserver resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/lbvserver? **view=summary**

Use this query-parameter to get the summary output of lbvserver resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/lbvserver? **pagesize=#no;pageno=#no**

Use this query-parameter to get the lbvserver resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "lbvserver": [ {

"name":<String_value>,

"insertvserveripport":<String_value>,

"vipheader":<String_value>,

"value":<String_value>,

"ip":<String_value>,

"ipv46":<String_value>,

"ippattern":<String_value>,

"ipmask":<String_value>,

"listenpolicy":<String_value>,

"listenpriority":<Integer_value>,

"ipmapping":<String_value>,

"port":<Integer_value>,

"ipset":<String_value>,

"range":<Integer_value>,
```

```
"servicetype":<String_value>,

"ngname":<String_value>,

"type":<String_value>,

"curstate":<String_value>,

"effectivestate":<String_value>,

"status":<Integer_value>,

"lbrrreason":<Integer_value>,

"redirect":<String_value>,

"precedence":<String_value>,

"redirurl":<String_value>,

"authentication":<String_value>,

"authn401":<String_value>,

"authnvsname":<String_value>,

"homepage":<String_value>,

"dnsvservername":<String_value>,

"domain":<String_value>,

"servicename":<String_value>,

"weight":<Integer_value>,

"cachevserver":<String_value>,

"backupvserver":<String_value>,

"clttimeout":<Integer_value>,

"somethod":<String_value>,
```

```
"sopersistence":<String_value>,

"sopersistencetimeout":<Integer_value>,

"healththreshold":<Integer_value>,

"sothreshold":<Integer_value>,

"sobackupaction":<String_value>,

"lbmethod":<String_value>,

"backuplbmethod":<String_value>,

"hashlength":<Integer_value>,

"dataoffset":<Integer_value>,

"health":<Integer_value>,

"datalength":<Integer_value>,

"netmask":<String_value>,

"v6netmasklen":<Integer_value>,

"rule":<String_value>,

"resrule":<String_value>,

"ruletype":<Integer_value>,

"groupname":<String_value>,

"m":<String_value>,

"tosid":<Integer_value>,

"persistencetype":<String_value>,

"timeout":<Integer_value>,

"cookiedomain":<String_value>,
```

```
"persistmask":<String_value>,

"v6persistmasklen":<Integer_value>,

"persistencebackup":<String_value>,

"backuppersistencetimeout":<Integer_value>,

"cacheable":<String_value>,

"rtspnat":<String_value>,

"sessionless":<String_value>,

"trofspersistence":<String_value>,

"map":<String_value>,

"connfailover":<String_value>,

"redirectportrewrite":<String_value>,

"downstateflush":<String_value>,

"disableprimaryondown":<String_value>,

"gt2gb":<String_value>,

"consolidatedlconn":<String_value>,

"consolidatedlconngbl":<String_value>,

"thresholdvalue":<Integer_value>,

"bindpoint":<String_value>,

"cookiename":<String_value>,

"version":<Integer_value>,

"totalservices":<Integer_value>,

"activeservices":<Integer_value>,
```

```
"statechangetimesec":<String_value>,

"statechangetimeseconds":<Integer_value>,

"statechangetimemsec":<Integer_value>,

"tickssincelaststatechange":<Integer_value>,

"authenticationhost":<String_value>,

"push":<String_value>,

"pushvserver":<String_value>,

"pushlabel":<String_value>,

"pushmulticlients":<String_value>,

"tcpprofilename":<String_value>,

"httpprofilename":<String_value>,

"dbprofilename":<String_value>,

"aigwprofilename":<String_value>,

"mcpprofilename":<String_value>,

"comment":<String_value>,

"l2conn":<String_value>,

"oracleserverversion":<String_value>,

"mssqlserverversion":<String_value>,

"mysqlprotocolversion":<Integer_value>,

"mysqlserverversion":<String_value>,

"mysqlcharacterset":<Integer_value>,

"mysqlservercapabilities":<Integer_value>,
```

```
"appflowlog":<String_value>,

"netprofile":<String_value>,

"isgslb":<Boolean_value>,

"icmpvsrresponse":<String_value>,

"rhistate":<String_value>,

"newservicerequest":<Integer_value>,

"newservicerequestunit":<String_value>,

"newservicerequestincrementinterval":<Integer_value>,

"persistavpno":<Integer[]_value>,

"skippersistency":<String_value>,

"td":<Integer_value>,

"minautoscalemembers":<Integer_value>,

"maxautoscalemembers":<Integer_value>,

"authnprofile":<String_value>,

"macmoderetainvlan":<String_value>,

"dbslb":<String_value>,

"dns64":<String_value>,

"bypassaaaa":<String_value>,

"recursionavailable":<String_value>,

"processlocal":<String_value>,

"vsvrdynconnsothreshold":<Integer_value>,

"backupvserverstatus":<String_value>,
```

```
"dnsprofilename":<String_value>,

"lbprofilename":<String_value>,

"redirectfromport":<Integer_value>,

"httpsredirecturl":<String_value>,

"retainconnectionsoncluster":<String_value>,

"nodefaultbindings":<String_value>,

"adfsproxyprofile":<String_value>,

"tcpprobeport":<Integer_value>,

"quicbridgeprofilename":<String_value>,

"probeprotocol":<String_value>,

"probeport":<Integer_value>,

"probesuccessresponsecode":<String_value>,

"quicprofilename":<String_value>,

"order":<Integer_value>,

"toggleorder":<String_value>,

"orderthreshold":<Integer_value>,

"currentactiveorder":<String_value>,

"apiprofile":<String_value>,

"dnsoverhttps":<String_value>,

"wasmmodule":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

get

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver/ name_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/lbvserver/ name_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/lbvserver/ name_value<String> ? **view=summary**

Use this query-parameter to get the summary output of lbvserver resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lbvserver": [ {

"name":<String_value>,

"insertvserveripport":<String_value>,

"vipheader":<String_value>,
```

```
"value":<String_value>,

"ip":<String_value>,

"ipv46":<String_value>,

"ippattern":<String_value>,

"ipmask":<String_value>,

"listenpolicy":<String_value>,

"listenpriority":<Integer_value>,

"ipmapping":<String_value>,

"port":<Integer_value>,

"ipset":<String_value>,

"range":<Integer_value>,

"servicetype":<String_value>,

"ngname":<String_value>,

"type":<String_value>,

"curstate":<String_value>,

"effectivestate":<String_value>,

"status":<Integer_value>,

"lbrrreason":<Integer_value>,

"redirect":<String_value>,

"precedence":<String_value>,

"redirurl":<String_value>,

"authentication":<String_value>,
```

```
"authn401":<String_value>,

"authnvsname":<String_value>,

"homepage":<String_value>,

"dnsvservername":<String_value>,

"domain":<String_value>,

"servicename":<String_value>,

"weight":<Integer_value>,

"cachevserver":<String_value>,

"backupvserver":<String_value>,

"clttimeout":<Integer_value>,

"somethod":<String_value>,

"sopersistence":<String_value>,

"sopersistencetimeout":<Integer_value>,

"healththreshold":<Integer_value>,

"sothreshold":<Integer_value>,

"sobackupaction":<String_value>,

"lbmethod":<String_value>,

"backuplbmethod":<String_value>,

"hashlength":<Integer_value>,

"dataoffset":<Integer_value>,

"health":<Integer_value>,

"datalength":<Integer_value>,
```

```
"netmask":<String_value>,

"v6netmasklen":<Integer_value>,

"rule":<String_value>,

"resrule":<String_value>,

"ruletype":<Integer_value>,

"groupname":<String_value>,

"m":<String_value>,

"tosid":<Integer_value>,

"persistencetype":<String_value>,

"timeout":<Integer_value>,

"cookiedomain":<String_value>,

"persistmask":<String_value>,

"v6persistmasklen":<Integer_value>,

"persistencebackup":<String_value>,

"backuppersistencetimeout":<Integer_value>,

"cacheable":<String_value>,

"rtspnat":<String_value>,

"sessionless":<String_value>,

"trofspersistence":<String_value>,

"map":<String_value>,

"connfailover":<String_value>,

"redirectportrewrite":<String_value>,
```

```
"downstateflush":<String_value>,

"disableprimaryondown":<String_value>,

"gt2gb":<String_value>,

"consolidatedlconn":<String_value>,

"consolidatedlconngbl":<String_value>,

"thresholdvalue":<Integer_value>,

"bindpoint":<String_value>,

"cookiename":<String_value>,

"version":<Integer_value>,

"totalservices":<Integer_value>,

"activeservices":<Integer_value>,

"statechangetimesec":<String_value>,

"statechangetimeseconds":<Integer_value>,

"statechangetimemsec":<Integer_value>,

"tickssincelaststatechange":<Integer_value>,

"authenticationhost":<String_value>,

"push":<String_value>,

"pushvserver":<String_value>,

"pushlabel":<String_value>,

"pushmulticlients":<String_value>,

"tcpprofilename":<String_value>,

"httpprofilename":<String_value>,
```

```
"dbprofilename":<String_value>,

"aigwprofilename":<String_value>,

"mcpprofilename":<String_value>,

"comment":<String_value>,

"l2conn":<String_value>,

"oracleserverversion":<String_value>,

"mssqlserverversion":<String_value>,

"mysqlprotocolversion":<Integer_value>,

"mysqlserverversion":<String_value>,

"mysqlcharacterset":<Integer_value>,

"mysqlservercapabilities":<Integer_value>,

"appflowlog":<String_value>,

"netprofile":<String_value>,

"isgslb":<Boolean_value>,

"icmpvsrresponse":<String_value>,

"rhistate":<String_value>,

"newservicerequest":<Integer_value>,

"newservicerequestunit":<String_value>,

"newservicerequestincrementinterval":<Integer_value>,

"persistavpno":<Integer[]_value>,

"skippersistency":<String_value>,

"td":<Integer_value>,
```

```
"minautoscalemembers":<Integer_value>,

"maxautoscalemembers":<Integer_value>,

"authnprofile":<String_value>,

"macmoderetainvlan":<String_value>,

"dbslb":<String_value>,

"dns64":<String_value>,

"bypassaaaa":<String_value>,

"recursionavailable":<String_value>,

"processlocal":<String_value>,

"vsvrdynconnsothreshold":<Integer_value>,

"backupvserverstatus":<String_value>,

"dnsprofilename":<String_value>,

"lbprofilename":<String_value>,

"redirectfromport":<Integer_value>,

"httpsredirecturl":<String_value>,

"retainconnectionsoncluster":<String_value>,

"nodefaultbindings":<String_value>,

"adfsproxyprofile":<String_value>,

"tcpprobeport":<Integer_value>,

"quicbridgeprofilename":<String_value>,

"probeprotocol":<String_value>,

"probeport":<Integer_value>,
```

```
"probesuccessresponsecode":<String_value>,

"quicprofilename":<String_value>,

"order":<Integer_value>,

"toggleorder":<String_value>,

"orderthreshold":<Integer_value>,

"currentactiveorder":<String_value>,

"apiprofile":<String_value>,

"dnsoverhttps":<String_value>,

"wasmmodule":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

count

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "lbvserver": [ { "__count": "#no"} ] }
```

lbvserver_service_binding

Binding object showing the service that can be bound to lbvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
weight	<Integer>	Read-write	Weight to assign to the specified service. Minimum value = 1 Maximum value = 100
servicegroupname	<String>	Read-write	Name of the service group. Minimum length = 1
name	<String>	Read-write	Name for the virtual server. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric, underscore, hash (#), period (.), space, colon (:), at sign (@), equal sign (=), and hyphen (-) characters. Can be changed after the virtual server is created.

CLI Users: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my vserver" or 'my vserver'). .

Minimum length = 1

Minimum value = 1

Maximum value = 8192

Minimum length = 1

Possible values = UP, DOWN, UNKNOWN, BUSY, OUT OF SERVICE, GOING OUT OF SERVICE, DOWN WHEN GOING OUT OF SERVICE, NS_EMPTY_STR, Unknown, DISABLED

Range 1 - 65535

* in CLI is represented as 65535 in NITRO API

Possible values = HTTP, FTP, TCP, UDP, SSL, SSL_BRIDGE, SSL_TCP, DTLS, NNTP, DNS, DHCPRA, ANY, SIP_UDP, SIP_TCP, SIP_SSL, DNS_TCP, RTSP, PUSH, SSL_PUSH, RADIUS, RDP, MYSQL, MSSQL, DIAMETER, SSL_DIAMETER, TFTP, ORACLE, SMPP, SYSLOGTCP, SYSLOGUDP, FIX, SSL_FIX, PROXY, USER_TCP, USER_SSL_TCP, QUIC, IPFIX, LOGSTREAM, MONGO, MONGO_TLS, MQTT, MQTT_TLS, QUIC_BRIDGE, HTTP_QUIC, DOT, SSL_PROXY, KAFKA_PRODUCER

Range 1 - 65535

* in CLI is represented as 65535 in NITRO API

Operations

(click to see Properties)

- ADD
- DELETE
- GET
- GET (ALL)
- COUNT

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

add

URL: http:// <netscaler-ip-address /nitro/v1/config/lbvserver_service_binding **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{

"lbvserver_service_binding":{

<b>"name":<String_value>,
```

```
</b>"servicename":<String_value>,

"weight":<Integer_value>,

"servicegroupname":<String_value>,

"order":<Integer_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

delete

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_service_binding/ name_value<String> **Query-parameters: args** http:// <netscaler-ip-address> /nitro/v1/config/ lbvserver_service_binding/ name_value<String> ? **args=servicename: <String_value> ,servicegroupname: <String_value>**

HTTP Method: DELETE

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

get

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_service_binding/ name_value<String> **Query-parameters: filter** http:// <netscaler-ip-address> /nitro/v1/config/ lbvserver_service_binding/ name_value<String> ? **filter=property-name1:property-value1,property-name2:property-value2**

Use this query-parameter to get the filtered set of lbvserver_service_binding resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

pagination http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_service_binding/ name_value<String> ? **pagesize=#no;pageno=#no**

Use this query-parameter to get the lbvserver_service_binding resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lbvserver_service_binding": [ {

"weight":<Integer_value>,

"servicegroupname":<String_value>,

"name":<String_value>,

"order":<Integer_value>,

"servicename":<String_value>,

"vserverid":<String_value>,

"curstate":<String_value>,

"port":<Integer_value>,

"servicetype":<String_value>,
```

```
"preferredlocation":<String_value>,

"ipv46":<String_value>,

"vsvrbindsvcip":<String_value>,

"dynamicweight":<Integer_value>,

"cookieipport":<String_value>,

"vsvrbindsvcport":<Integer_value>,

"cookiename":<String_value>,

"orderstr":<String_value>

}]}
```

get (all)

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_service_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_service_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "lbvserver_service_binding": [ {

"weight":<Integer_value>,

"servicegroupname":<String_value>,

"name":<String_value>,

"order":<Integer_value>,

"servicename":<String_value>,

"vserverid":<String_value>,

"curstate":<String_value>,

"port":<Integer_value>,

"servicetype":<String_value>,

"preferredlocation":<String_value>,

"ipv46":<String_value>,

"vsvrbindsvcip":<String_value>,

"dynamicweight":<Integer_value>,

"cookieipport":<String_value>,

"vsvrbindsvcport":<Integer_value>,

"cookiename":<String_value>,

"orderstr":<String_value>

}]}
```

count

URL: http:// <netscaler-ip-address> /nitro/v1/config/lbvserver_service_binding/ name_value<String> ? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{"lbvserver_service_binding": [ { "__count": "#no"} ] }
```

sslcertkey

Configuration for certificate key resource.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
certkey	<String>	Read-write	Name for the certificate and private-key pair. Must begin with an ASCII alphanumeric or underscore (_) character, and must contain only ASCII alphanumeric,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			underscore, hash (#), period (.), space, colon (:), at (@), equals (=), and hyphen (-) characters. Cannot be changed after the certificate-key pair is created. The following requirement applies only to the Citrix ADC CLI: If the name includes one or more spaces, enclose the name in double or single quotation marks (for example, "my cert" or 'my cert'). Minimum length = 1
cert	<String>	Read-write	Name of and, optionally, path to the X509 certificate file that is used to form the certificate-key pair. The certificate file should be present on the appliance's hard-disk drive or solid-state drive. Storing a certificate in any location other than the default might cause inconsistency

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			in a high availability setup. /nsconfig/ssl/ is the default path. Minimum length = 1
key	<String>	Read-write	Name of and, optionally, path to the private-key file that is used to form the certificate-key pair. The certificate file should be present on the appliance's hard-disk drive or solid-state drive. Storing a certificate in any location other than the default might cause inconsistency in a high availability setup. /nsconfig/ssl/ is the default path. Minimum length = 1
password	<Boolean>	Read-write	Passphrase that was used to encrypt the private-key. Use this option to load encrypted private-keys in PEM format.
fipskey	<String>	Read-write	Name of the FIPS key that was created inside the Hardware Security Module (HSM) of a FIPS appliance, or a key that was imported into the HSM. Minimum length = 1

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
hsmkey	<String>	Read-write	Name of the HSM key that was created in the External Hardware Security Module (HSM) of a FIPS appliance. Minimum length = 1
inform	<String>	Read-write	Input format of the certificate and the private-key files. The three formats supported by the appliance are: PEM - Privacy Enhanced Mail DER - Distinguished Encoding Rule PFX - Personal Information Exchange. Default value: PEM Possible values = DER, PEM, PFX
passplain	<String>	Read-write	Pass phrase used to encrypt the private-key. Required when adding an encrypted private-key in PEM format. Minimum length = 1
expirymonitor	<String>	Read-write	Issue an alert when the certificate is about to expire.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			Possible values = ENABLED, DISABLED
notificationperiod	<Integer>	Read-write	Time, in number of days, before certificate expiration, at which to generate an alert that the certificate is about to expire. Minimum value = 10 Maximum value = 100
bundle	<String>	Read-write	Parse the certificate chain as a single file after linking the server certificate to its issuer's certificate within the file. Default value: NO Possible values = YES, NO
deletecertkeyfilesonremoval	<String>	Read-write	This option is used to automatically delete certificate/key files from physical device when the added certkey is removed. When deleteCertKeyFilesOnRemoval option is used at rm certkey command, it overwrites the deleteCertKeyFilesOnRemoval setting

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			used at add/set certkey command. Default value: CERTKEYFILE_DELETE_NO Possible values = NO, ALWAYS, IF_EXPIRED
deletefromdevice	<Boolean>	Read-write	Delete cert/key file from file system.
linkcertkeyname	<String>	Read-write	Name of the Certificate Authority certificate-key pair to which to link a certificate-key pair. Minimum length = 1
nodomaincheck	<Boolean>	Read-write	Override the check for matching domain names during a certificate update operation.
ocspstaplingcache	<Boolean>	Read-write	Clear cached ocspStapling response in certkey.
signaturealg	<String>	Read-only	Signature algorithm.
certificatetype	<String[]>	Read-only	Specifies whether the certificate is of type root-CA, intermediate-CA, server, client, or client and server. Possible values = ROOT_CERT, INTM_CERT,

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			CLNT_CERT, SRVR_CERT, UNKNOWN_CERT
serial	<String>	Read-only	Serial number.
issuer	<String>	Read-only	Issuer name.
clientcertnotbefore	<String>	Read-only	Not-Before date.
clientcertnotafter	<String>	Read-only	Not-After date.
daystoexpiration	<Integer>	Read-only	Days remaining for the certificate to expire.
subject	<String>	Read-only	Subject name.
publickey	<String>	Read-only	Public key algorithm.
publickeysize	<Integer>	Read-only	Size of the public key.
version	<Integer>	Read-only	Version.
priority	<Integer>	Read-only	ocsp priority.
status	<String>	Read-only	Status of the certificate. Possible values = Valid, Not yet valid, Expired
passcrypt	<String>	Read-only	Passcrypt. Minimum length = 1
data	<Integer>	Read-only	Vserver Id.
servicename	<String>	Read-only	Service name to which the certificate key pair is bound.

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
sandns	<String>	Read-only	Subject Alternative Name (SAN) is an extension to X.509 that allows various values to be associated with a security certificate using a subjectAltName field. These values are called "Subject Alternative Names" (SAN). This field is for DNS names.
sanipadd	<String>	Read-only	Subject Alternative Name (SAN) is an extension to X.509 that allows various values to be associated with a security certificate using a subjectAltName field. These values are called "Subject Alternative Names" (SAN). This field is for IP address.
ocspresponsestatus	<String>	Read-only	Ocsp response status of the certificate. Possible values = NONE, EXPIRED, VALID

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
builtin	<String[]>	Read-only	Flag to determine if Cert key is built-in or not. Possible values = MODIFIABLE, DELETABLE, IMMUTABLE, PARTITION_ALL
feature	<String>	Read-only	The feature to be checked while applying this config.
certkeydigest	<String>	Read-only	Stores the added md5sum of certificate and key files.
certificatesource	<String>	Read-only	Location of the certificate. Default value: LOCAL Possible values = LOCAL, REMOTE
certkeystatus	<String>	Read-only	Status of the certkey in PE. Possible values = ACTIVE, INACTIVE(Default state), INACTIVE(No Private Key), INACTIVE(Duplicate SAN-Multiple clashing certs), INACTIVE(Duplicat

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
			e SAN-All SAN entires not covered), INACTIVE(Duplicate SAN-Earlier expiry), INACTIVE(Crossed MAX SAN limit), INACTIVE(No common name), INACTIVE(Common name/SAN too long), INACTIVE(No memory), INACTIVE(MAX cert req len reached), INACTIVE(X509 Name failure)
_nextgenapiresource	<String>	Read-only	.
__count	<Double>	Read-only	count parameter

Operations

(click to see Properties)

- ADD
- DELETE
- UPDATE
- UNSET
- LINK
- UNLINK
- GET (ALL)

- GET
- COUNT
- CHANGE
- CLEAR

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

add

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcertkey **HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"sslcertkey":{

<b>"certkey":<String_value>,

</b><b>"cert":<String_value>,

</b>"key":<String_value>,

"password":<Boolean_value>,

"fipskey":<String_value>,

"hsmkey":<String_value>,

"inform":<String_value>,

"passplain":<String_value>,

"expirymonitor":<String_value>,

"notificationperiod":<Integer_value>,

"bundle":<String_value>,

"deletecertkeyfilesonremoval":<String_value>

}}
```

Response: HTTP Status Code on Success: 201 Created

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

delete

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcertkey/ certkey_value<String> **Query-parameters: args=deletefromdevice: <Boolean_value> ,deletecertkeyfilesonremoval: <String_value>**

update

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcertkey **HTTP Method:** PUT

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"sslcertkey":{

<b>"certkey":<String_value>,

</b>"expirymonitor":<String_value>,

"notificationperiod":<Integer_value>,

"deletecertkeyfilesonremoval":<String_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

unset

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcertkey? **action=unset HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"sslcertkey":{

<b>"certkey":<String_value>,

</b>"expirymonitor":true,

"notificationperiod":true,

"deletecertkeyfilesonremoval":true

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

link

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcertkey? **action=link HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"sslcertkey":{

<b>"certkey":<String_value>,

</b><b>"linkcertkeyname":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

unlink

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcertkey? **action=unlink HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"sslcertkey":{

<b>"certkey":<String_value>

</b>}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

change

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcertkey? **action=update HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"sslcertkey":{

<b>"certkey":<String_value>,

</b>"cert":<String_value>,

"key":<String_value>,
```

```
"password":<Boolean_value>,

"fipskey":<String_value>,

"inform":<String_value>,

"passplain":<String_value>,

"nodomaincheck":<Boolean_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

clear

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcertkey? **action=clear HTTP Method:** POST

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Content-Type:application/json

Request Payload:

```
{"sslcertkey":{

<b>"certkey":<String_value>,

</b>"ocspstaplingcache":<Boolean_value>

}}
```

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

get (all)

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcertkey **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/sslcertkey? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

filter http:// <netscaler-ip-address> /nitro/v1/config/sslcertkey? **filter=property-name1:property-val1,property-name2:property-val2**

Use this query-parameter to get the filtered set of sslcertkey resources configured on NetScaler.Filtering can be done on any of the properties of the resource.

view http:// <netscaler-ip-address> /nitro/v1/config/sslcertkey? **view=summary**

Use this query-parameter to get the summary output of sslcertkey resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

pagination http:// <netscaler-ip-address> /nitro/v1/config/sslcertkey? **pagesize=#no;pageno=#no**

Use this query-parameter to get the sslcertkey resources in chunks.

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "sslcertkey": [ {

"certkey":<String_value>,

"cert":<String_value>,

"key":<String_value>,

"inform":<String_value>,

"signaturealg":<String_value>,

"certificatetype":<String[]_value>,

"serial":<String_value>,

"issuer":<String_value>,

"clientcertnotbefore":<String_value>,

"clientcertnotafter":<String_value>,

"daystoexpiration":<Integer_value>,

"subject":<String_value>,

"publickey":<String_value>,

"publickeysize":<Integer_value>,

"version":<Integer_value>,

"priority":<Integer_value>,

"status":<String_value>,

"fipskey":<String_value>,

"hsmkey":<String_value>,

"passcrypt":<String_value>,

"passplain":<String_value>,
```

```
"data":<Integer_value>,

"servicename":<String_value>,

"expirymonitor":<String_value>,

"notificationperiod":<Integer_value>,

"linkcertkeyname":<String_value>,

"sandns":<String_value>,

"sanipadd":<String_value>,

"ocspresponsestatus":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,

"certkeydigest":<String_value>,

"certificatesource":<String_value>,

"certkeystatus":<String_value>,

"deletecertkeyfilesonremoval":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

get

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcertkey/ certkey_value<String> **Query-parameters: attrs** http:// <netscaler-ip-address> /nitro/v1/config/sslcertkey/ certkey_value<String> ? **attrs=property-name1,property-name2**

Use this query parameter to specify the resource details that you want to retrieve.

view http:// <netscaler-ip-address> /nitro/v1/config/sslcertkey/ certkey_value<String> ? **view=summary**

Use this query-parameter to get the summary output of sslcertkey resources configured on NetScaler.

Note: By default, the retrieved results are displayed in detail view (?view=detail).

HTTP Method: GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{  "sslcertkey": [ {

"certkey":<String_value>,

"cert":<String_value>,

"key":<String_value>,

"inform":<String_value>,

"signaturealg":<String_value>,

"certificatetype":<String[]_value>,

"serial":<String_value>,

"issuer":<String_value>,

"clientcertnotbefore":<String_value>,
```

```
"clientcertnotafter":<String_value>,

"daystoexpiration":<Integer_value>,

"subject":<String_value>,

"publickey":<String_value>,

"publickeysize":<Integer_value>,

"version":<Integer_value>,

"priority":<Integer_value>,

"status":<String_value>,

"fipskey":<String_value>,

"hsmkey":<String_value>,

"passcrypt":<String_value>,

"passplain":<String_value>,

"data":<Integer_value>,

"servicename":<String_value>,

"expirymonitor":<String_value>,

"notificationperiod":<Integer_value>,

"linkcertkeyname":<String_value>,

"sandns":<String_value>,

"sanipadd":<String_value>,

"ocspresponsestatus":<String_value>,

"builtin":<String[]_value>,

"feature":<String_value>,
```

```
"certkeydigest":<String_value>,

"certificatesource":<String_value>,

"certkeystatus":<String_value>,

"deletecertkeyfilesonremoval":<String_value>,

"_nextgenapiresource":<String_value>

}]}
```

count

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslcertkey? **count=yes HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "sslcertkey": [ { "__count": "#no"} ] }
```

sslvserver_binding

Binding object which returns the resources bound to sslvserver.

Properties

(click to see Operations)

NAME	DATA TYPE	PERMISSIONS	DESCRIPTION
vservername	<String>	Read-write	Name of the SSL virtual server for which to show detailed information. Minimum length = 1
sslvserver_sslcacertbundle_binding	<sslvserver_sslcacertbundle_binding[]>	Read-only	sslcacertbundle that can be bound to sslvserver.
sslvserver_sslpolicy_binding	<sslvserver_sslpolicy_binding[]>	Read-only	sslpolicy that can be bound to sslvserver.
sslvserver_sslciphersuite_binding	<sslvserver_sslciphersuite_binding[]>	Read-only	sslciphersuite that can be bound to sslvserver.
sslvserver_sslcertkey_binding	<sslvserver_sslcertkey_binding[]>	Read-only	sslcertkey that can be bound to sslvserver.
sslvserver_sslcertkeybundle_binding	<sslvserver_sslcertkeybundle_binding[]>	Read-only	sslcertkeybundle that can be bound to sslvserver.
sslvserver_ecccurve_binding	<sslvserver_ecccurve_binding[]>	Read-only	ecccurve that can be bound to sslvserver.
sslvserver_hashicorp_binding	<sslvserver_hashicorp_binding[]>	Read-only	hashicorp that can be bound to sslvserver.
sslvserver_sslcipher_binding	<sslvserver_sslcipher_binding[]>	Read-only	sslcipher that can be bound to sslvserver.

Operations

(click to see Properties)

- GET
- GET (ALL)

Some options that you can use for each operations:

- **Getting warnings in response:** NITRO allows you to get warnings in an operation by specifying the 'warning' query parameter as 'yes'. For example, to get warnings while connecting to the NetScaler appliance, the URL is as follows:

  http:// <netscaler-ip-address> /nitro/v1/config/login?warning=yes

  If any, the warnings are displayed in the response payload with the HTTP code '209 X-NITRO-WARNING'.

- **Authenticated access for individual NITRO operations:** NITRO allows you to logon to the NetScaler appliance to perform individual operations. You can use this option instead of creating a NITRO session (using the login object) and then using that session to perform all operations,

  To do this, you must specify the username and password in the request header of the NITRO request as follows:

  X-NITRO-USER: <username>

  X-NITRO-PASS: <password>

  Note: In such cases, make sure that the request header DOES not include the following:

  Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

`*Note: *` Mandatory parameters are marked in red and placeholder content is marked in green

get

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslvserver_binding/ vservername_value<String> **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "sslvserver_binding": [ {

"vservername":<String_value>,

"sslvserver_sslciphersuite_binding":<sslvserver_sslciphersuite_binding[]_value>,

"sslvserver_sslpolicy_binding":<sslvserver_sslpolicy_binding[]_value>,

"sslvserver_ecccurve_binding":<sslvserver_ecccurve_binding[]_value>,

"sslvserver_hashicorp_binding":<sslvserver_hashicorp_binding[]_value>,

"sslvserver_sslcertkey_binding":<sslvserver_sslcertkey_binding[]_value>,

"sslvserver_sslcacertbundle_binding":<sslvserver_sslcacertbundle_binding[]_value>,

"sslvserver_sslcertkeybundle_binding":<sslvserver_sslcertkeybundle_binding[]_value>,

"sslvserver_sslcipher_binding":<sslvserver_sslcipher_binding[]_value>

}]}
```

get (all)

URL: http:// <netscaler-ip-address> /nitro/v1/config/sslvserver_binding **HTTP Method:** GET

Request Headers:

Cookie:NITRO_AUTH_TOKEN= <tokenvalue>

Accept:application/json

Query-parameters: bulkbindings http:// <netscaler-ip-address> /nitro/v1/config/ sslvserver_binding? **bulkbindings=yes**

NITRO allows you to fetch bindings in bulk.

Note: get (all) method can be used only in conjuction with bulkbindings query parameter.

Response: HTTP Status Code on Success: 200 OK

HTTP Status Code on Failure: 4xx <string> (for general HTTP errors) or 5xx <string> (for NetScaler-specific errors). The response payload provides details of the error

Response Header:

Content-Type:application/json

Response Payload:

```
{ "sslvserver_binding": [ {

"vservername":<String_value>,

"sslvserver_sslciphersuite_binding":<sslvserver_sslciphersuite_binding[]_value>,

"sslvserver_sslpolicy_binding":<sslvserver_sslpolicy_binding[]_value>,

"sslvserver_ecccurve_binding":<sslvserver_ecccurve_binding[]_value>,

"sslvserver_hashicorp_binding":<sslvserver_hashicorp_binding[]_value>,

"sslvserver_sslcertkey_binding":<sslvserver_sslcertkey_binding[]_value>,

"sslvserver_sslcacertbundle_binding":<sslvserver_sslcacertbundle_binding[]_value>,

"sslvserver_sslcertkeybundle_binding":<sslvserver_sslcertkeybundle_binding[]_value>,

"sslvserver_sslcipher_binding":<sslvserver_sslcipher_binding[]_value>

}]}
```